NCIPE - Jone and Antonio		National Critical Information Infrastructure Protection CentreCommon Vulnerabilities and Exposures(CVE) Report01 - 15 Sep 2021Vol. 08 No. 17					
Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID		
			Application				
30lines							
rentpress							
Improper Neutralizati on of Input During Web Page Generation ('Cross-site Scripting')	09-Sep-21	4.3	The RentPress WordPress plugin is vulnerable to Reflected Cross-Site Scripting via the selections parameter found in the ~/src/rentPress/AjaxReques ts.php file which allows attackers to inject arbitrary web scripts, in versions up to and including 6.6.4.	N/A	A-30L-RENT- 170921/1		
			CVE ID : CVE-2021-38323				
adaptivescal	e						
lxdui							
Use of Hard- coded Credentials	03-Sep-21	10	A Hardcoded JWT Secret Key in metadata.py in AdaptiveScale LXDUI through 2.1.3 allows attackers to gain admin access to the host system. CVE ID : CVE-2021-40494	N/A	A-ADA-LXDU- 170921/2		
addtoany	I			L			
addtoany_share_buttons							
Improper Neutralizati on of Input During Web Page Generation ('Cross-site	06-Sep-21	3.5	The AddToAny Share Buttons WordPress plugin before 1.7.46 does not sanitise its Sharing Header setting when outputting it in frontend pages, allowing high privilege users such as admin to	N/A	A-ADD-ADDT- 170921/3		
CVSS Scoring Sc	ale 0-1	1-2	2-3 3-4 4-5 5-6	6-7 7-8	8-9 9-10		

Scripting')perform Cross-Site Scripting attacks even when the unfiltered_html capability is disallowed CVE ID : CVE-2021-24568perform Cross-Site Scripting attacks even when the unfiltered_html capability is disallowed CVE ID : CVE-2021-24568Adobe acrobatAcrobat Reader DC versions versions 2020.013.20074 (and earlier), 2020.001.30018 (and earlier) and 2017.011.30188 (and earlier) are affected by an Out-of-bounds Write vulnerability in the CoolType abitrary. 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-2021-21086https://helpx achec.om/s ecurity/prod ucts/acrobat/ apsb21- 09.htmlAADO-ACRO- travel AADO-ACRO- travelOut-of- bounds Write02-Sep-216.8Acrobat Reader DC versions versions 2020.013.20074 (and earlier), 2020.001.30018 (and earlier) and 2017.011.30188 (and earlier), 2020.01.30018 (and earlier) and 2017.011.30189 adobe.com/s ecurity/prod ucts/acrobat/ abobc.com/s ecurity/prod ucts/acrobat/ an Out-of-bounds Write winerability in the CoolType library. An unauthenticated an Out-of-bounds Write winerability in the CoolType library. An unauthenticated an Out-of-bounds Write winerability in the CoolType library. An unauthenticated attacker could leverage this winerability in the CoolType library. An unauthenticated attacker could leverage this winerability in the CoolType library. An unauthenticated attacker could leverage this undershilty in the coolType library. An unauthenticated attacker could leverage this unoto-founds Wri	Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Adobeacrobatacrobat0ut-of- bounds Write02-Sep-216.8Acrobat Reader DC versions versions 2020.013.20074 (and earlier), 2020.001.30018 (and earlier) and 2017.011.30188 (and earlier) are affected by an Out-of-bounds Write vulnerability in the CoolType library. 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://helpx a.dobe.com/s ccurity/prod ucts/acrobat/ apsb21- 09.htmlA-AD0-ACR0- 170921/4Out-of- bounds02-Sep-216.8Acrobat Reader DC versions versions 2020.013.20074 (and earlier), 2020.001.30018 (and earlier) and 2017.011.30188 (and earlier), 2020.001.30018 (and earlier) and 2017.011.30188 (and earlier), adobe.com/s ecurity/prod ucts/acrobat/ adobe.com/s ecurity/prod ucts/acrobat/ adobe.com/s ecurity/prod ucts/acrobat/ adobe.com/s ecurity/prod ucts/acrobat/ adobe.com/s ecurity/prod ucts/acrobat/ adobe.com/s ecurity/prod ucts/acrobat/ adobe.com/s ecurity/prod ucts/acrobat/ adobe.com/s ecurity/prod ucts/acrobat/ adobe.com/s ecurity/prod ucts/acrobat/ adobe.com/s ecurity/prod ucts/acrobat/ adobe.com/s ecurity/prod ucts/acrobat/ adobe.com/s ecurity/prod ucts/acrobat/ adobe.com/s ecurity/prod ucts/acrobat/ adobe.com/s ecurity/prod ucts/acrobat/ adobe.com/s ecurity/prod ucts/acrobat/ adobe.com/s ecurity/prod ucts/acrobat/ adobe.com/s ecurity/prod ucts/acrobat/ adobe.com/s ecurity/prod ucts/acrobat/ adobe.com/s ecurity/prod ucts	Scripting')			attacks even when the unfiltered_html capability is		
acrobatOut-of- bounds Write02-Sep-216.8Acrobat Reader DC versions versions 2020.013.20074 				CVE ID : CVE-2021-24568		
Out-of- bounds02-Sep-21Acrobat Reader DC versions versions 2020.013.20074 (and earlier), 2020.001.30018 (and earlier) and 2017.011.30188 (and earlier) are affected by an Out-of-bounds Write vulnerability in the CoolType library. An unauthenticated attacker could leverage this yulnerability 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://helpx adobe.com/s ecurity/prod ucts/acrobat/ apsb21- 09.htmlA-ADO-ACRO- 170921/4Out-of- bounds02-Sep-21Acrobat Reader DC versions versions 2020.013.20074 (and earlier), 2020.001.30018 (and earlier) and 2017.011.30188 (and earlier), adobe.com/s ecurity/prod ucts/acrobat/ apsb21- 09.htmlhttps://helpx a.adobe.com/s ecurity/prod ucts/acrobat/ apsb21- 09.htmlOut-of- bounds Write02-Sep-216.8Acrobat Reader DC versions versions 2020.013.20074 (and earlier), 2020.001.30018 (and earlier) and 2017.011.30188 ecurity/prod ucts/acrobat/ apsb21- 09.htmlA-ADO-ACRO- 170921/5	Adobe					
Out-of- bounds Write02-Sep-21estableversions 2020.013.20074 (and earlier), 2020.001.30018 (and earlier) and 2017.011.30188 (and earlier) are affected by an Out-of-bounds Write uherability in the CoolType library. An unauthenticated attacker could leverage this yuherability to achieve arbitrary code execution in here context of the current user. Exploitation of this issue requires user interaction in that a victim must open a malicious file.https://helpx achieve apsb21- 09.htmlA-ADO-ACRO- 170921/4Out-of- bounds02-Sep-21estable estableAcrobat Reader DC versions versions 2020.013.20074 (and earlier), 2020.001.30018 (and earlier) and 2017.011.30188 adobe.com/s ecurity/prod ucts/acrobat/https://helpx achoe.com/s ecurity/prod ucts/acrobat/Out-of- bounds02-Sep-21estable estableAcrobat Reader DC versions versions 2020.013.20074 (and earlier), 2020.001.30018 (and earlier) and 2017.011.30188 adobe.com/s ecurity/prod ucts/acrobat/https://helpx achoe.com/s ecurity/prod ucts/acrobat/Out-of- bounds02-Sep-21estable estableAcrobat Reader DC versions versions 2020.013.20074 (and earlier), achoe.com/s ecurity/prod ucts/acrobat/https://helpx achoe.com/s ecurity/prod ucts/acrobat/Out-of- boundsestableAcrobat Reader DC versions (and earlier), achoe.com/s ecurity/prod ucts/acrobat/Achoo-ACRO- 170921/5Out-of- boundsestableAchoo-Acrobat achoe.com/s ecurity/prod ucts/acrobat/Achoo-Acrobat achoe.com/s ecurity/prod ucts/acrobat/Out-of- bounds	acrobat					
Out-of- bounds Write02-Sep-216.8Acrobat Reader DC versions versions 2020.013.20074 (and earlier), 2020.001.30018 (and earlier) and 2017.011.30188 an Out-of-bounds Write vulnerability in the CoolType library. An unauthenticated attacker could leverage thishttps://helpx adobe.com/s ecurity/prod apsb21- 09.htmlA-ADO-ACRO- 170921/5	bounds Write	02-Sep-21	6.8	versions 2020.013.20074 (and earlier), 2020.001.30018 (and earlier) and 2017.011.30188 (and earlier) are affected by an Out-of-bounds Write vulnerability in the CoolType library. 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.	.adobe.com/s ecurity/prod ucts/acrobat/ apsb21-	
Out-of- bounds Write02-Sep-216.8versions 2020.013.20074 (and earlier), 2020.001.30018 (and (and earlier) and 2017.011.30188 (and earlier) are affected by an Out-of-bounds Writehttps://helpx .adobe.com/s ecurity/prod ucts/acrobat/A-ADO-ACRO- 170921/5Ibrary. An unauthenticated attacker could leverage thisapsb21- 09.html09.html	acrobat_dc					
arbitrary code execution in	bounds	02-Sep-21	6.8	versions 2020.013.20074 (and earlier), 2020.001.30018 (and earlier) and 2017.011.30188 (and earlier) are affected by an Out-of-bounds Write vulnerability in the CoolType library. An unauthenticated attacker could leverage this vulnerability to achieve	.adobe.com/s ecurity/prod ucts/acrobat/ apsb21-	

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			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-2021-21086		
acrobat_read	ler				
Out-of- bounds Write	02-Sep-21	6.8	Acrobat Reader DC versions versions 2020.013.20074 (and earlier), 2020.001.30018 (and earlier) and 2017.011.30188 (and earlier) are affected by an Out-of-bounds Write vulnerability in the CoolType library. 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-2021-21086	https://helpx .adobe.com/s ecurity/prod ucts/acrobat/ apsb21- 09.html	A-ADO-ACRO- 170921/6
acrobat_read	ler_dc			<u> </u>	L
Out-of- bounds Write	02-Sep-21	6.8	Acrobat Reader DC versions versions 2020.013.20074 (and earlier), 2020.001.30018 (and earlier) and 2017.011.30188 (and earlier) are affected by an Out-of-bounds Write vulnerability in the CoolType library. An unauthenticated attacker could leverage this vulnerability to achieve arbitrary code execution in	https://helpx .adobe.com/s ecurity/prod ucts/acrobat/ apsb21- 09.html	A-ADO-ACRO- 170921/7

CVSS Scoring Scale	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10
Page 3 of 1/17/										

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			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-2021-21086		
adobe_comm	erce		CVE ID : CVE-2021-21086		
auobe_comm			Magento Commerce versions		
N/A	01-Sep-21	4	2.4.2 (and earlier), 2.4.2-p1 (and earlier) and 2.3.7 (and earlier) are affected by a business logic error in the placeOrder graphql mutation. An authenticated attacker can leverage this vulnerability to altar the price of an item. CVE ID : CVE-2021-36012	https://helpx .adobe.com/s ecurity/prod ucts/magento /apsb21- 64.html	A-ADO-ADOB- 170921/8
XML Injection (aka Blind XPath Injection)	01-Sep-21	7.5	Magento Commerce versions 2.4.2 (and earlier), 2.4.2-p1 (and earlier) and 2.3.7 (and earlier) are affected by an XML Injection vulnerability in the 'City' field. An unauthenticated attacker can trigger a specially crafted script to achieve remote code execution. CVE ID : CVE-2021-36020	https://helpx .adobe.com/s ecurity/prod ucts/magento /apsb21- 64.html	A-ADO-ADOB- 170921/9
Improper Neutralizati on of Special Elements in Output Used by a Downstrea m Component	01-Sep-21	6.5	Magento Commerce versions 2.4.2 (and earlier), 2.4.2-p1 (and earlier) and 2.3.7 (and earlier) are affected by an XML Injection vulnerability in the Widgets Update Layout. An attacker with admin privileges can trigger a specially crafted script to	https://helpx .adobe.com/s ecurity/prod ucts/magento /apsb21- 64.html	A-ADO-ADOB- 170921/10

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
('Injection')			achieve remote code execution.		
			CVE ID : CVE-2021-36022		
Improper Neutralizati on of Special Elements used in an OS Command ('OS Command Injection')	01-Sep-21	6.5	Magento Commerce versions 2.4.2 (and earlier), 2.4.2-p1 (and earlier) and 2.3.7 (and earlier) are affected by an Improper Neutralization of Special Elements Used In A Command via the Data collection endpoint. An attacker with admin privileges can upload a specially crafted file to achieve remote code execution.	https://helpx .adobe.com/s ecurity/prod ucts/magento /apsb21- 64.html	A-ADO-ADOB- 170921/11
			CVE ID : CVE-2021-36024		
Improper Input Validation	01-Sep-21	6.5	Magento Commerce versions 2.4.2 (and earlier), 2.4.2-p1 (and earlier) and 2.3.7 (and earlier) are affected by an improper input validation vulnerability while saving a customer's details with a specially crafted file. An authenticated attacker with admin privileges can leverage this vulnerability to achieve remote code execution.	https://helpx .adobe.com/s ecurity/prod ucts/magento /apsb21- 64.html	A-ADO-ADOB- 170921/12
			CVE ID : CVE-2021-36025		
Improper Neutralizati on of Input During Web Page Generation ('Cross-site	01-Sep-21	4.3	Magento Commerce versions 2.4.2 (and earlier), 2.4.2-p1 (and earlier) and 2.3.7 (and earlier) are affected by a stored cross-site scripting vulnerability in the customer address upload feature that	https://helpx .adobe.com/s ecurity/prod ucts/magento /apsb21- 64.html	A-ADO-ADOB- 170921/13

0-1

1-2

2-3

4-5

6-7

5-6

7-8

8-9

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Scripting')			could be abused by an attacker to inject malicious scripts into vulnerable form fields. Malicious JavaScript may be executed in a victim's browser when they browse to the page containing the vulnerable field. CVE ID : CVE-2021-36026		
Improper Neutralizati on of Input During Web Page Generation ('Cross-site Scripting')	01-Sep-21	4.3	Magento Commerce versions 2.4.2 (and earlier), 2.4.2-p1 (and earlier) and 2.3.7 (and earlier) are affected by a stored cross-site scripting vulnerability that could be abused by an attacker to inject malicious scripts into vulnerable form fields. Malicious JavaScript may be executed in a victim's browser when they browse to the page containing the vulnerable field. CVE ID : CVE-2021-36027	https://helpx .adobe.com/s ecurity/prod ucts/magento /apsb21- 64.html	A-ADO-ADOB- 170921/14
XML Injection (aka Blind XPath Injection)	01-Sep-21	6.5	Magento Commerce versions 2.4.2 (and earlier), 2.4.2-p1 (and earlier) and 2.3.7 (and earlier) are affected by an XML Injection vulnerability when saving a configurable product. An attacker with admin privileges can trigger a specially crafted script to achieve remote code execution. CVE ID : CVE-2021-36028	https://helpx .adobe.com/s ecurity/prod ucts/magento /apsb21- 64.html	A-ADO-ADOB- 170921/15
Improper Authorizatio	01-Sep-21	6.5	Magento Commerce versions 2.4.2 (and earlier), 2.4.2-p1	https://helpx .adobe.com/s	A-ADO-ADOB- 170921/16
CVSS Scoring Sco	ale 0-1	1-2	2-3 3-4 4-5 5-6	6-7 7-8	8-9 9-10

 3-4
 4-5
 5-6
 6-7

 Page 6 of 1474

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
n			(and earlier) and 2.3.7 (and earlier) are affected by an improper improper authorization vulnerability. An attacker with admin privileges could leverage this vulnerability to achieve remote code execution. CVE ID : CVE-2021-36029	ecurity/prod ucts/magento /apsb21- 64.html	
Improper Input Validation	01-Sep-21	5	Magento Commerce versions 2.4.2 (and earlier), 2.4.2-p1 (and earlier) and 2.3.7 (and earlier) are affected by an improper input validation vulnerability during the checkout process. An unauthenticated attacker can leverage this vulnerability to alter the price of items. CVE ID : CVE-2021-36030	https://helpx .adobe.com/s ecurity/prod ucts/magento /apsb21- 64.html	A-ADO-ADOB- 170921/17
Improper Limitation of a Pathname to a Restricted Directory ('Path Traversal')	01-Sep-21	6.5	Magento Commerce versions 2.4.2 (and earlier), 2.4.2-p1 (and earlier) and 2.3.7 (and earlier) are affected by a Path Traversal vulnerability via the `theme[preview_image]` parameter. An attacker with admin privileges could leverage this vulnerability to achieve remote code execution. CVE ID : CVE-2021-36031	https://helpx .adobe.com/s ecurity/prod ucts/magento /apsb21- 64.html	A-ADO-ADOB- 170921/18
Improper Input Validation	01-Sep-21	6.5	Magento Commerce versions 2.4.2 (and earlier), 2.4.2-p1 (and earlier) and 2.3.7 (and earlier) are affected by an improper input validation vulnerability. An	https://helpx .adobe.com/s ecurity/prod ucts/magento /apsb21- 64.html	A-ADO-ADOB- 170921/19
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
			authenticated attacker can trigger an insecure direct object reference in the `V1/customers/me` endpoint to achieve information exposure and privilege escalation.		
			CVE ID : CVE-2021-36032		
XML Injection (aka Blind XPath Injection)	01-Sep-21	6.5	Magento Commerce versions 2.4.2 (and earlier), 2.4.2-p1 (and earlier) and 2.3.7 (and earlier) are affected by an XML Injection vulnerability in the Widgets Module. An attacker with admin privileges can trigger a specially crafted script to achieve remote code execution. CVE ID : CVE-2021-36033	https://helpx .adobe.com/s ecurity/prod ucts/magento /apsb21- 64.html	A-ADO-ADOB- 170921/20
Improper Input Validation	01-Sep-21	6.5	Magento Commerce versions 2.4.2 (and earlier), 2.4.2-p1 (and earlier) and 2.3.7 (and earlier) are affected by an improper input validation vulnerability. An attacker with admin privileges can upload a specially crafted file to achieve remote code execution. CVE ID : CVE-2021-36034	https://helpx .adobe.com/s ecurity/prod ucts/magento /apsb21- 64.html	A-ADO-ADOB- 170921/21
Improper Input Validation	01-Sep-21	6.5	Magento Commerce versions 2.4.2 (and earlier), 2.4.2-p1 (and earlier) and 2.3.7 (and earlier) are affected by an improper input validation vulnerability. An attacker with admin privileges could	https://helpx .adobe.com/s ecurity/prod ucts/magento /apsb21- 64.html	A-ADO-ADOB- 170921/22

0-1

2-3

1-2

4-5

6-7

5-6

7-8

8-9

9-10

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			make a crafted request to the Adobe Stock API to achieve remote code execution. CVE ID : CVE-2021-36035		
Incorrect Authorizatio n	01-Sep-21	4	CVE ID : CVE-2021-30033Magento Commerce versions2.4.2 (and earlier), 2.4.2-p1(and earlier) and 2.3.7 (andearlier) are affected by animproper improperauthorization vulnerability.An authenticated attackercould leverage thisvulnerability to achievesensitive informationdisclosure.CVE ID : CVE-2021-36037	https://helpx .adobe.com/s ecurity/prod ucts/magento /apsb21- 64.html	A-ADO-ADOB- 170921/23
Improper Input Validation	01-Sep-21	4	Magento Commerce versions 2.4.2 (and earlier), 2.4.2-p1 (and earlier) and 2.3.7 (and earlier) are affected by an improper input validation vulnerability in the Multishipping Module. An authenticated attacker could leverage this vulnerability to achieve sensitive information disclosure. CVE ID : CVE-2021-36038	https://helpx .adobe.com/s ecurity/prod ucts/magento /apsb21- 64.html	A-ADO-ADOB- 170921/24
Incorrect Authorizatio n	01-Sep-21	4	Magento Commerce versions 2.4.2 (and earlier), 2.4.2-p1 (and earlier) and 2.3.7 (and earlier) are affected by an improper input validation vulnerability via the `quoteId` parameter. An attacker can abuse this vulnerability to disclose sensitive information.	https://helpx .adobe.com/s ecurity/prod ucts/magento /apsb21- 64.html	A-ADO-ADOB- 170921/25
CVSS Scoring Sc	ale 0-1	1-2	2-3 3-4 4-5 5-6	6-7 7-8	8-9 9-10

3-44-55-6Page 9 of 1474

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2021-36039		
Improper Input Validation	01-Sep-21	6.5	Magento Commerce versions 2.4.2 (and earlier), 2.4.2-p1 (and earlier) and 2.3.7 (and earlier) are affected by an improper input validation vulnerability. An attacker with admin privileges can upload a specially crafted file to bypass file extension restrictions and could lead to remote code execution. CVE ID : CVE-2021-36040	https://helpx .adobe.com/s ecurity/prod ucts/magento /apsb21- 64.html	A-ADO-ADOB- 170921/26
Improper Input Validation	01-Sep-21	6.5	Magento Commerce versions 2.4.2 (and earlier), 2.4.2-p1 (and earlier) and 2.3.7 (and earlier) are affected by an improper input validation vulnerability. An attacker with admin privileges could upload a specially crafted file in the 'pub/media` directory could lead to remote code execution. CVE ID : CVE-2021-36041	https://helpx .adobe.com/s ecurity/prod ucts/magento /apsb21- 64.html	A-ADO-ADOB- 170921/27
Improper Input Validation	01-Sep-21	6.5	Magento Commerce versions 2.4.2 (and earlier), 2.4.2-p1 (and earlier) and 2.3.7 (and earlier) are affected by an improper input validation vulnerability in the API File Option Upload Extension. An attacker with Admin privileges can achieve unrestricted file upload which can result in remote code execution. CVE ID : CVE-2021-36042	https://helpx .adobe.com/s ecurity/prod ucts/magento /apsb21- 64.html	A-ADO-ADOB- 170921/28
CVSS Scoring Sc	cale 0-1	1-2	2-3 3-4 4-5 5-6	6-7 7-8	8-9 9-10

3-4 4-5 Page 10 of 1474

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Server-Side Request Forgery (SSRF)	01-Sep-21	6	Magento Commerce versions 2.4.2 (and earlier), 2.4.2-p1 (and earlier) and 2.3.7 (and earlier) are affected by a blind SSRF vulnerability in the bundled dotmailer extension. An attacker with admin privileges could abuse this to achieve remote code execution should Redis be enabled. CVE ID : CVE-2021-36043	https://helpx .adobe.com/s ecurity/prod ucts/magento /apsb21- 64.html	A-ADO-ADOB- 170921/29
Improper Input Validation	01-Sep-21	5	Magento Commerce versions 2.4.2 (and earlier), 2.4.2-p1 (and earlier) and 2.3.7 (and earlier) are affected by an improper input validation vulnerability. An unauthenticated attacker could abuse this vulnerability to cause a server-side denial- of-service using a GraphQL field. CVE ID : CVE-2021-36044	https://helpx .adobe.com/s ecurity/prod ucts/magento /apsb21- 64.html	A-ADO-ADOB- 170921/30
after_effects		<u> </u>			
Improper Neutralizati on of Special Elements used in an OS Command ('OS Command Injection')	08-Sep-21	7.6	Adobe After Effects version 18.1 (and earlier) is affected by a potential Command injection vulnerability when chained with a development and debugging tool for JavaScript scripts. 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	https://helpx .adobe.com/e e/security/pr oducts/after_ effects/apsb2 1-33.html	A-ADO-AFTE- 170921/31
CVSS Scoring Sc	ale 0-1	1-2	2-3 3-4 4-5 5-6 Page 11 of 1474	6-7 7-8	8-9 9-10

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			interaction in that a victim must open a malicious file.		
			CVE ID : CVE-2021-28571		
Out-of- bounds Write	02-Sep-21	6.8	Adobe After Effects version 18.2.1 (and earlier) is affected by an out-of-bounds Write vulnerability when parsing a specially crafted 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://helpx .adobe.com/s ecurity/prod ucts/after_eff ects/apsb21- 54.html	A-ADO-AFTE- 170921/32
			CVE ID : CVE-2021-35993		
Out-of- bounds Write	02-Sep-21	9.3	Adobe After Effects version 18.2.1 (and earlier) is affected by an out-of-bounds Write vulnerability when parsing a specially crafted 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-2021-35994	https://helpx .adobe.com/s ecurity/prod ucts/after_eff ects/apsb21- 54.html	A-ADO-AFTE- 170921/33
Improper Input Validation	02-Sep-21	4.3	Adobe After Effects version 18.2.1 (and earlier) is affected by an Improper input validation vulnerability when parsing a specially	https://helpx .adobe.com/s ecurity/prod ucts/after_eff ects/apsb21-	A-ADO-AFTE- 170921/34

CVSS Scoring Scale	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10
			Г	2 - 3 - 12 - 3	f 1/7/					

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			crafted file. An unauthenticated attacker could leverage this vulnerability to disclose arbitrary memory information 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-2021-35995	54.html	
Access of Memory Location After End of Buffer	02-Sep-21	9.3	Adobe After Effects version 18.2.1 (and earlier) is affected by a memory corruption vulnerability when parsing a specially crafted 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-2021-35996	https://helpx .adobe.com/s ecurity/prod ucts/after_eff ects/apsb21- 54.html	A-ADO-AFTE- 170921/35
Improper Restriction of Operations within the Bounds of a Memory Buffer	02-Sep-21	9.3	Adobe After Effects version 18.2.1 (and earlier) is affected by a memory corruption vulnerability when parsing a specially crafted file. An unauthenticated attacker could leverage this vulnerability to achieve arbitrary code execution in the context of the current user. Exploitation of this	https://helpx .adobe.com/s ecurity/prod ucts/after_eff ects/apsb21- 54.html	A-ADO-AFTE- 170921/36
CVSS Scoring Sc	ale 0-1	1-2	2-3 3-4 4-5 5-6	6-7 7-8	8-9 9-10

Page 13 of 1474

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			issue requires user interaction in that a victim must open a malicious file.		
			CVE ID : CVE-2021-36017		
Out-of- bounds Read	02-Sep-21	4.3	Adobe After Effects version 18.2.1 (and earlier) is affected by an Out-of-bounds Read vulnerability when parsing a specially crafted file. An unauthenticated attacker could leverage this vulnerability to disclose sensitive memory information in the context of the current user. Exploitation of this issue requires user interaction in that a victim must open a malicious file.	https://helpx .adobe.com/s ecurity/prod ucts/after_eff ects/apsb21- 54.html	A-ADO-AFTE- 170921/37
			CVE ID : CVE-2021-36018		
Out-of- bounds Read	02-Sep-21	4.3	Adobe After Effects version 18.2.1 (and earlier) is affected by an Out-of-bounds Read vulnerability when parsing a specially crafted file. An unauthenticated attacker could leverage this vulnerability to disclose arbitrary memory information 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-2021-36019	https://helpx .adobe.com/s ecurity/prod ucts/after_eff ects/apsb21- 54.html	A-ADO-AFTE- 170921/38
bridge					
Improper Restriction of	01-Sep-21	9.3	Adobe Bridge version 11.1 (and earlier) is affected by a memory corruption	https://helpx .adobe.com/s ecurity/prod	A-ADO-BRID- 170921/39
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 & CVE ID	Patch	NCIIPC ID
Operations within the Bounds of a Memory Buffer			vulnerability due to insecure handling of a malicious Bridge 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-2021-39816	ucts/bridge/ apsb21- 69.html	
Improper Restriction of Operations within the Bounds of a Memory Buffer	01-Sep-21	9.3	Adobe Bridge version 11.1 (and earlier) is affected by a memory corruption vulnerability due to insecure handling of a malicious Bridge 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-2021-39817	https://helpx .adobe.com/s ecurity/prod ucts/bridge/ apsb21- 69.html	A-ADO-BRID- 170921/40
Access of Memory Location After End of Buffer	01-Sep-21	9.3	Adobe Bridge version 11.1 (and earlier) is affected by a memory corruption vulnerability due to insecure handling of a malicious Bridge 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-2021-36049	https://helpx .adobe.com/s ecurity/prod ucts/bridge/ apsb21- 69.html	A-ADO-BRID- 170921/41
Improper Restriction of Operations within the	01-Sep-21	9.3	Adobe Bridge version 11.1 (and earlier) is affected by a memory corruption vulnerability due to insecure handling of a malicious	https://helpx .adobe.com/s ecurity/prod ucts/bridge/ apsb21-	A-ADO-BRID- 170921/42

CVSS Scoring Scale	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9
			F	Page 15 of	f 1474				

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Bounds of a Memory Buffer			Bridge 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-2021-36059	69.html	
Improper Restriction of Operations within the Bounds of a Memory Buffer	01-Sep-21	9.3	Adobe Bridge version 11.1 (and earlier) is affected by a memory corruption vulnerability due to insecure handling of a malicious Bridge 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-2021-36067	https://helpx .adobe.com/s ecurity/prod ucts/bridge/ apsb21- 69.html	A-ADO-BRID- 170921/43
Improper Restriction of Operations within the Bounds of a Memory Buffer	01-Sep-21	9.3	Adobe Bridge version 11.1 (and earlier) is affected by a memory corruption vulnerability due to insecure handling of a malicious Bridge 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-2021-36068	https://helpx .adobe.com/s ecurity/prod ucts/bridge/ apsb21- 69.html	A-ADO-BRID- 170921/44
Improper Restriction of Operations within the Bounds of a Memory	01-Sep-21	9.3	Adobe Bridge version 11.1 (and earlier) is affected by a memory corruption vulnerability due to insecure handling of a malicious Bridge file, potentially resulting in arbitrary code	https://helpx .adobe.com/s ecurity/prod ucts/bridge/ apsb21- 69.html	A-ADO-BRID- 170921/45

0-1

1-2

6-7

5-6

7-8

8-9

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Buffer			execution in the context of the current user. User interaction is required to exploit this vulnerability. CVE ID : CVE-2021-36069		
Out-of- bounds Read	01-Sep-21	4.3	Adobe Bridge versions 11.1 (and earlier) are affected by an out-of-bounds read vulnerability that could lead to disclosure of arbitrary memory. An attacker could leverage this vulnerability to bypass mitigations such as ASLR. Exploitation of this issue requires user interaction in that a victim must open a malicious file. CVE ID : CVE-2021-36071	https://helpx .adobe.com/s ecurity/prod ucts/bridge/ apsb21- 69.html	A-ADO-BRID- 170921/46
Out-of- bounds Write	01-Sep-21	9.3	Adobe Bridge versions 11.1 (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 file. CVE ID : CVE-2021-36072	https://helpx .adobe.com/s ecurity/prod ucts/bridge/ apsb21- 69.html	A-ADO-BRID- 170921/47
Out-of- bounds Write	01-Sep-21	9.3	Adobe Bridge version 11.1 (and earlier) is affected by a heap-based buffer overflow vulnerability when parsing a crafted .SGI file. An attacker could leverage this vulnerability to execute code in the context of the current user. Exploitation of this	https://helpx .adobe.com/s ecurity/prod ucts/bridge/ apsb21- 69.html	A-ADO-BRID- 170921/48

CVSS	Scoring	Scale
Cv 33	JCOING	Juic

0-1

1-2

5-6

6-7

7-8

8-9

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			issue requires user interaction in that a victim must open a malicious file. CVE ID : CVE-2021-36073		
Out-of- bounds Read	01-Sep-21	4.3	Adobe Bridge versions 11.1 (and earlier) are affected by an out-of-bounds read vulnerability that could lead to disclosure of arbitrary memory. An attacker could leverage this vulnerability to bypass mitigations such as ASLR. Exploitation of this issue requires user interaction in that a victim must open a malicious file. CVE ID : CVE-2021-36074	https://helpx .adobe.com/s ecurity/prod ucts/bridge/ apsb21- 69.html	A-ADO-BRID- 170921/49
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	01-Sep-21	9.3	Adobe Bridge version 11.1 (and earlier) is affected by a Buffer Overflow vulnerability due to insecure handling of a malicious Bridge 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-2021-36075	https://helpx .adobe.com/s ecurity/prod ucts/bridge/ apsb21- 69.html	A-ADO-BRID- 170921/50
Improper Restriction of Operations within the Bounds of a Memory Buffer	01-Sep-21	9.3	Adobe Bridge version 11.1 (and earlier) is affected by a memory corruption vulnerability due to insecure handling of a malicious Bridge file, potentially resulting in arbitrary code execution in the context of the current user. User	https://helpx .adobe.com/s ecurity/prod ucts/bridge/ apsb21- 69.html	A-ADO-BRID- 170921/51

0-1

1-2

2-3 3-4

4-5

6-7

5-6

7-8

8-9

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			interaction is required to exploit this vulnerability.		
			CVE ID : CVE-2021-36076		
Improper Restriction of Operations within the Bounds of a Memory Buffer	01-Sep-21	4.3	Adobe Bridge version 11.1 (and earlier) is affected by a memory corruption vulnerability due to insecure handling of a malicious SVG file, potentially resulting in local application denial of service in the context of the current user. User interaction is required to exploit this vulnerability. CVE ID : CVE-2021-36077	https://helpx .adobe.com/s ecurity/prod ucts/bridge/ apsb21- 69.html	A-ADO-BRID- 170921/52
Improper Restriction of Operations within the Bounds of a Memory Buffer	01-Sep-21	9.3	Adobe Bridge version 11.1 (and earlier) is affected by a memory corruption vulnerability due to insecure handling of a malicious Bridge 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-2021-36078	https://helpx .adobe.com/s ecurity/prod ucts/bridge/ apsb21- 69.html	A-ADO-BRID- 170921/53
Out-of- bounds Read	01-Sep-21	9.3	Adobe Bridge version 11.1 (and earlier) is affected by an out-of-bounds read vulnerability when parsing a crafted .SGI file, which could result in a read past the end of an allocated memory structure. An attacker could leverage this vulnerability to execute code in the context of the current user. Exploitation	https://helpx .adobe.com/s ecurity/prod ucts/bridge/ apsb21- 69.html	A-ADO-BRID- 170921/54

[CVSS Scoring Scale	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10
-											

CaptivateAdobe Captivate version interaction in that a victim must open a malicious file. CVE D: CVE 2021-36079captivateCaptivateCreation of Temporary File in Directory with Insscure PermissionsAdobe Captivate version 11.5.5 (and earlier) is affected by an Creation of Temporary File In Directory with Incorrect Permissions unerability that could result in privilege escalation in the context of the current user. The attacker must plant analicious file in a particular. Instance: Networkhttps://helpx adobe.com/s ecurity/prod ucts/captivat e/apsb21- 60.htmlConnect	Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Creation of Temporary File in Directory with nescure Permissions01-Sep-214.4Adobe Captivate version affected by an Creation of Temporary File In Directory with Incorrect Permissions vulnerability that could result in privilege escalation in the context of the current user. The attacker must plant a malcious file in a particular location of the victim's machine. Exploitation of this issue requires user interaction in that a victim must launch the Captivate Installer.https://helpx. adobe.com/s ecurity/prod ucts/captivat e/apsb21- 60.htmlA-ADO-CAPT- ucts/captivat e/apsb21- 60.htmlViolation of Secure Design Principles01-Sep-214.3Adobe Connect version 11.2.2 (and earlier) is affected by a secure design principles violation vulnerability via the 'pbMode' parameter. An umathenticated attacker could leverage this vulnerability to edit or delete recordings on the Connect ervironment. Exploitation of this issue requires user interaction in that a victim must publish a link of ahttps://helpx adobe.com/s ecurity/prod ucts/captivat ecurity/prod ucts/captivat ecurity/prod				interaction in that a victim must open a malicious file.		
Creation of Temporary File in Directory11.5.5 (and earlier) is affected by an Creation of Temporary File In Directory With Incorrect Permissionshttps://helpx adobe.com/s ecurity/prod utes/capivation of the context of the current user. The attacker must plant analicious file in a particular location of the victim's machine. Exploitation of this issue requires user interaction in that a victim must launch the Captivate Installer.https://helpx adobe.com/s ecurity/prod (apsb21- 60.htmlAADO-CAPT- user. The attacker must plant adobe.com/s ecurity/prod (apsb21- 60.htmlA-ADO-CAPT- user. The attacker (apsb21- 60.htmlConnectViolation of 1.2.2 (and earlier) is affected by a secure design vulnerability via the 'pbMode' parameter. An unauthenticated attacker could leverage this vulnerability to edit or delete recordings on the Connect (apsb21- 66.htmlA-ADO-CONN- user.Violation of Secure Design Principles11.5.2 (and earlier) is affected by a secure design vulnerability via the 'pbMode' parameter. An unauthenticated attacker could leverage this vulnerability to edit or delete recordings on the Connect (apsb21- 66.htmlA-ADO-CONN- users/interview	captivate					
Violation of Secure Design Principles01-Sep-21Adobe Connect version 11.2.2 (and earlier) is affected by a secure design principles violation vulnerability via the 'pbMode' parameter. An unauthenticated attacker could leverage this vulnerability to edit or delete recordings on the Connect environment. Exploitation of this issue requires user interaction in that a victim must publish a link of ahttps://helpx adobe.com/s ecurity/prod ucts/connect /apsb21- 66.htmlA-ADO-CONN- 170921/56	Temporary File in Directory with Insecure	01-Sep-21	4.4	11.5.5 (and earlier) is affected by an Creation of Temporary File In Directory With Incorrect Permissions vulnerability that could result in privilege escalation in the context of the current user. The attacker must plant a malicious file in a particular location of the victim's machine. Exploitation of this issue requires user interaction in that a victim must launch the Captivate Installer.	.adobe.com/s ecurity/prod ucts/captivat e/apsb21-	
Violation of Secure Design Principles11.2.2 (and earlier) is affected by a secure design principles violation vulnerability via the 'pbMode' parameter. An unauthenticated attacker could leverage this vulnerability to edit or delete recordings on the Connect environment. Exploitation of this issue requires user interaction in that a victim must publish a link of ahttps://helpx adobe.com/s ecurity/prod https://helpx adobe.com/s ecurity/prod (apsb21- 66.htmlA-ADO-CONN- adobe.com/s	connect					
	Secure Design	01-Sep-21	4.3	11.2.2 (and earlier) is affected by a secure design principles violation vulnerability via the 'pbMode' parameter. An unauthenticated attacker could leverage this vulnerability to edit or delete recordings on the Connect environment. Exploitation of this issue requires user interaction in that a victim must publish a link of a	.adobe.com/s ecurity/prod ucts/connect /apsb21-	

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2021-36061		
Improper Neutralizati on of Input During Web Page Generation ('Cross-site Scripting')	01-Sep-21	4.3	Adobe Connect version 11.2.2 (and earlier) is affected by a Reflected Cross- site Scripting vulnerability that could be abused by an attacker to inject malicious scripts into vulnerable form fields. 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. CVE ID : CVE-2021-36062	https://helpx .adobe.com/s ecurity/prod ucts/connect /apsb21- 66.html	A-ADO-CONN- 170921/57
Improper Neutralizati on of Input During Web Page Generation ('Cross-site Scripting')	01-Sep-21	4.3	Adobe Connect version 11.2.2 (and earlier) is affected by a Reflected Cross- site Scripting vulnerability that could be abused by an attacker to inject malicious scripts into vulnerable form fields. Malicious JavaScript may be executed in a victim's browser when they browse to the page containing the vulnerable field. CVE ID : CVE-2021-36063	https://helpx .adobe.com/s ecurity/prod ucts/connect /apsb21- 66.html	A-ADO-CONN- 170921/58
creative_clou	ıd				
Uncontrolle d Search Path Element	08-Sep-21	4.4	Adobe Creative Cloud Desktop 3.5 (and earlier) is affected by an uncontrolled search path vulnerability that could result in elevation of privileges. Exploitation of this issue requires user interaction in that a victim	https://helpx .adobe.com/s ecurity/prod ucts/creative - cloud/apsb21 -31.html	A-ADO-CREA- 170921/59

CVSS Scoring Scale	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10
			F	Page 21 of	f 1474					

Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID		
		must log on to the attacker's				
		CVE ID : CVE-2021-28581				
vice			1	1		
08-Sep-21	6.9	version 7.1 (and earlier) is affected by an Insecure file permission vulnerability during installation process. A local authenticated attacker could leverage this vulnerability to achieve privilege escalation in the context of the current user.	https://helpx .adobe.com/s ecurity/prod ucts/integrity _service/apsb 21-27.html	A-ADO-GENU- 170921/60		
		CVE ID : CVE-2021-28568				
illustrator						
08-Sep-21	9.3	Adobe Illustrator version 25.2 (and earlier) is affected by a memory corruption vulnerability when parsing a specially crafted file. An unauthenticated attacker could leverage this vulnerability to disclose sensitive memory information 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-2021-21103	https://helpx .adobe.com/s ecurity/prod ucts/illustrat or/apsb21- 24.html	A-ADO-ILLU- 170921/61		
08-Sep-21	9.3	Adobe Illustrator version 25.2 (and earlier) is affected by a memory corruption vulnerability when parsing a specially crafted file. An unauthenticated attacker could leverage this	https://helpx .adobe.com/s ecurity/prod ucts/illustrat or/apsb21- 24.html	A-ADO-ILLU- 170921/62		
	rice 08-Sep-21 08-Sep-21	initial initial vice 6.9 08-Sep-21 6.9 08-Sep-21 9.3 08-Sep-21 9.3	Image: Constraint of the sector of the sec	Image: Note of the set of th		

			vulnerability to remote 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-2021-21104		
Access of Memory Location After End of Buffer	08-Sep-21	9.3	Adobe Illustrator version 25.2 (and earlier) is affected by a memory corruption vulnerability when parsing a specially crafted file. An unauthenticated attacker could leverage this vulnerability to achieve remote 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-2021-21105	https://helpx .adobe.com/s ecurity/prod ucts/illustrat or/apsb21- 24.html	A-ADO-ILLU- 170921/63
magento_ope	n_source				
N/A	01-Sep-21	4	Magento Commerce versions 2.4.2 (and earlier), 2.4.2-p1 (and earlier) and 2.3.7 (and earlier) are affected by a business logic error in the placeOrder graphql mutation. An authenticated attacker can leverage this vulnerability to altar the price of an item. CVE ID : CVE-2021-36012	https://helpx .adobe.com/s ecurity/prod ucts/magento /apsb21- 64.html	A-ADO-MAGE- 170921/64
XML Injection (aka Blind XPath	01-Sep-21	7.5	Magento Commerce versions 2.4.2 (and earlier), 2.4.2-p1 (and earlier) and 2.3.7 (and earlier) are affected by an	https://helpx .adobe.com/s ecurity/prod ucts/magento	A-ADO-MAGE- 170921/65

Page 23 of 1474

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Injection)			XML Injection vulnerability in the 'City' field. An unauthenticated attacker can trigger a specially crafted script to achieve remote code execution.	/apsb21- 64.html	
			CVE ID : CVE-2021-36020		
Improper Neutralizati on of Special Elements in Output Used by a Downstrea m Component ('Injection')	01-Sep-21	6.5	Magento Commerce versions 2.4.2 (and earlier), 2.4.2-p1 (and earlier) and 2.3.7 (and earlier) are affected by an XML Injection vulnerability in the Widgets Update Layout. An attacker with admin privileges can trigger a specially crafted script to achieve remote code execution.	https://helpx .adobe.com/s ecurity/prod ucts/magento /apsb21- 64.html	A-ADO-MAGE- 170921/66
			CVE ID : CVE-2021-36022		
Improper Neutralizati on of Special Elements used in an OS Command ('OS Command Injection')	01-Sep-21	6.5	Magento Commerce versions 2.4.2 (and earlier), 2.4.2-p1 (and earlier) and 2.3.7 (and earlier) are affected by an Improper Neutralization of Special Elements Used In A Command via the Data collection endpoint. An attacker with admin privileges can upload a specially crafted file to achieve remote code execution. CVE ID : CVE-2021-36024	https://helpx .adobe.com/s ecurity/prod ucts/magento /apsb21- 64.html	A-ADO-MAGE- 170921/67
Improper Input Validation	01-Sep-21	6.5	Magento Commerce versions 2.4.2 (and earlier), 2.4.2-p1 (and earlier) and 2.3.7 (and earlier) are affected by an improper input validation	https://helpx .adobe.com/s ecurity/prod ucts/magento /apsb21-	A-ADO-MAGE- 170921/68

CVSS Scoring Scale	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10
			F	Page 24 of	f 1474					

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			vulnerability while saving a customer's details with a specially crafted file. An authenticated attacker with admin privileges can leverage this vulnerability to achieve remote code execution.	64.html	
Improper Neutralizati on of Input During Web Page Generation ('Cross-site Scripting')	01-Sep-21	4.3	CVE ID : CVE-2021-36025 Magento Commerce versions 2.4.2 (and earlier), 2.4.2-p1 (and earlier) and 2.3.7 (and earlier) are affected by a stored cross-site scripting vulnerability in the customer address upload feature that could be abused by an attacker to inject malicious scripts into vulnerable form fields. Malicious JavaScript may be executed in a victim's browser when they browse to the page containing the vulnerable field. CVE ID : CVE-2021-36026	https://helpx .adobe.com/s ecurity/prod ucts/magento /apsb21- 64.html	A-ADO-MAGE- 170921/69
Improper Neutralizati on of Input During Web Page Generation ('Cross-site Scripting')	01-Sep-21	4.3	Magento Commerce versions 2.4.2 (and earlier), 2.4.2-p1 (and earlier) and 2.3.7 (and earlier) are affected by a stored cross-site scripting vulnerability that could be abused by an attacker to inject malicious scripts into vulnerable form fields. Malicious JavaScript may be executed in a victim's browser when they browse to the page containing the vulnerable field.	https://helpx .adobe.com/s ecurity/prod ucts/magento /apsb21- 64.html	A-ADO-MAGE- 170921/70
CVSS Scoring Sco	ale 0-1	1-2	2-3 3-4 4-5 5-6 Page 25 of 1474	6-7 7-8	8-9 9-10

Page 25 of 1474

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2021-36027		
XML Injection (aka Blind XPath Injection)	01-Sep-21	6.5	Magento Commerce versions 2.4.2 (and earlier), 2.4.2-p1 (and earlier) and 2.3.7 (and earlier) are affected by an XML Injection vulnerability when saving a configurable product. An attacker with admin privileges can trigger a specially crafted script to achieve remote code execution. CVE ID : CVE-2021-36028	https://helpx .adobe.com/s ecurity/prod ucts/magento /apsb21- 64.html	A-ADO-MAGE- 170921/71
Improper Authorizatio n	01-Sep-21	6.5	Magento Commerce versions 2.4.2 (and earlier), 2.4.2-p1 (and earlier) and 2.3.7 (and earlier) are affected by an improper improper authorization vulnerability. An attacker with admin privileges could leverage this vulnerability to achieve remote code execution. CVE ID : CVE-2021-36029	https://helpx .adobe.com/s ecurity/prod ucts/magento /apsb21- 64.html	A-ADO-MAGE- 170921/72
Improper Input Validation	01-Sep-21	5	Magento Commerce versions 2.4.2 (and earlier), 2.4.2-p1 (and earlier) and 2.3.7 (and earlier) are affected by an improper input validation vulnerability during the checkout process. An unauthenticated attacker can leverage this vulnerability to alter the price of items. CVE ID : CVE-2021-36030	https://helpx .adobe.com/s ecurity/prod ucts/magento /apsb21- 64.html	A-ADO-MAGE- 170921/73
Improper Limitation of a	01-Sep-21	6.5	Magento Commerce versions 2.4.2 (and earlier), 2.4.2-p1 (and earlier) and 2.3.7 (and	https://helpx .adobe.com/s ecurity/prod	A-ADO-MAGE- 170921/74
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	Descriptio	on & CVE I	D	Pa	tch	NCI	IPC ID
Pathname to a Restricted Directory ('Path Traversal')			earlier) are aff Traversal vuln the `theme[pre parameter. An admin privileg leverage this v achieve remote execution. CVE ID : CVE-2	erability eview_im attacker ges could ulnerabi e code	via age]` with lity to	ucts/m /apsb2 64.htm			
Improper Input Validation	01-Sep-21	6.5	Magento Comr 2.4.2 (and earl (and earlier) a earlier) are aff improper inpuvulnerability. A authenticated of trigger an inse object reference `V1/customers to achieve info exposure and p escalation. CVE ID : CVE-2	ier), 2.4.2 nd 2.3.7 ected by it validat An attacker cure dire ce in the s/me` en ormation privilege	2-p1 (and an ion can ect dpoint	https:/ .adobe. ecurity ucts/m /apsb2 64.htm	com/s /prod agento 1-	A-AD0 17092	9-MAGE- 1/75
XML Injection (aka Blind XPath Injection)	01-Sep-21	6.5	Magento Commerce versions 2.4.2 (and earlier), 2.4.2-p1 (and earlier) and 2.3.7 (and earlier) are affected by an XML Injection vulnerability in the Widgets Module. An attacker with admin privileges can trigger a specially crafted script to achieve remote code execution. CVE ID : CVE-2021-36033			https:/ .adobe. ecurity ucts/m /apsb2 64.htm	com/s /prod agento 1-	A-ADC 17092	9-MAGE- 1/76
Improper Input Validation	01-Sep-21	6.5	Magento Comr 2.4.2 (and earl (and earlier) a	https:/ .adobe. ecurity	com/s	A-ADC 17092	-MAGE- 1/77		
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 & CVE ID	Patch	NCIIPC ID
			earlier) are affected by an improper input validation vulnerability. An attacker with admin privileges can upload a specially crafted file to achieve remote code execution.	ucts/magento /apsb21- 64.html	
			CVE ID : CVE-2021-36034		
Improper Input Validation	01-Sep-21	6.5	Magento Commerce versions 2.4.2 (and earlier), 2.4.2-p1 (and earlier) and 2.3.7 (and earlier) are affected by an improper input validation vulnerability. An attacker with admin privileges could make a crafted request to the Adobe Stock API to achieve remote code execution. CVE ID : CVE-2021-36035	https://helpx .adobe.com/s ecurity/prod ucts/magento /apsb21- 64.html	A-ADO-MAGE- 170921/78
Incorrect Authorizatio n	01-Sep-21	4	Magento Commerce versions 2.4.2 (and earlier), 2.4.2-p1 (and earlier) and 2.3.7 (and earlier) are affected by an improper improper authorization vulnerability. An authenticated attacker could leverage this vulnerability to achieve sensitive information disclosure. CVE ID : CVE-2021-36037	https://helpx .adobe.com/s ecurity/prod ucts/magento /apsb21- 64.html	A-ADO-MAGE- 170921/79
Improper Input Validation	01-Sep-21	4	Magento Commerce versions 2.4.2 (and earlier), 2.4.2-p1 (and earlier) and 2.3.7 (and earlier) are affected by an improper input validation vulnerability in the Multishipping Module. An	https://helpx .adobe.com/s ecurity/prod ucts/magento /apsb21- 64.html	A-ADO-MAGE- 170921/80

CVSS	Scoring	Scale
0.00	00001116	ocure

0-1

1-2

5-6

6-7

7-8

8-9

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			authenticated attacker could leverage this vulnerability to achieve sensitive information disclosure. CVE ID : CVE-2021-36038		
Incorrect Authorizatio n	01-Sep-21	4	Magento Commerce versions 2.4.2 (and earlier), 2.4.2-p1 (and earlier) and 2.3.7 (and earlier) are affected by an improper input validation vulnerability via the `quoteId` parameter. An attacker can abuse this vulnerability to disclose sensitive information. CVE ID : CVE-2021-36039	https://helpx .adobe.com/s ecurity/prod ucts/magento /apsb21- 64.html	A-ADO-MAGE- 170921/81
Improper Input Validation	01-Sep-21	6.5	Magento Commerce versions 2.4.2 (and earlier), 2.4.2-p1 (and earlier) and 2.3.7 (and earlier) are affected by an improper input validation vulnerability. An attacker with admin privileges can upload a specially crafted file to bypass file extension restrictions and could lead to remote code execution. CVE ID : CVE-2021-36040	https://helpx .adobe.com/s ecurity/prod ucts/magento /apsb21- 64.html	A-ADO-MAGE- 170921/82
Improper Input Validation	01-Sep-21	6.5	Magento Commerce versions 2.4.2 (and earlier), 2.4.2-p1 (and earlier) and 2.3.7 (and earlier) are affected by an improper input validation vulnerability. An attacker with admin privileges could upload a specially crafted file in the 'pub/media' directory could lead to remote code	https://helpx .adobe.com/s ecurity/prod ucts/magento /apsb21- 64.html	A-ADO-MAGE- 170921/83

 CVSS Scoring Scale
 0-1
 1-2
 2-3
 3-4
 4-5
 5-6
 6-7
 7-8

 Page 29 of 1474

8-9

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID	
			execution.			
			CVE ID : CVE-2021-36041			
Improper Input Validation	01-Sep-21	6.5	Magento Commerce versions 2.4.2 (and earlier), 2.4.2-p1 (and earlier) and 2.3.7 (and earlier) are affected by an improper input validation vulnerability in the API File Option Upload Extension. An attacker with Admin privileges can achieve unrestricted file upload which can result in remote code execution.	https://helpx .adobe.com/s ecurity/prod ucts/magento /apsb21- 64.html	A-ADO-MAGE- 170921/84	
			CVE ID : CVE-2021-36042			
Server-Side Request Forgery (SSRF)	01-Sep-21	6	Magento Commerce versions 2.4.2 (and earlier), 2.4.2-p1 (and earlier) and 2.3.7 (and earlier) are affected by a blind SSRF vulnerability in the bundled dotmailer extension. An attacker with admin privileges could abuse this to achieve remote code execution should Redis be enabled. CVE ID : CVE-2021-36043	https://helpx .adobe.com/s ecurity/prod ucts/magento /apsb21- 64.html	A-ADO-MAGE- 170921/85	
Improper Input Validation	01-Sep-21	5	Magento Commerce versions 2.4.2 (and earlier), 2.4.2-p1 (and earlier) and 2.3.7 (and earlier) are affected by an improper input validation vulnerability. An unauthenticated attacker could abuse this vulnerability to cause a server-side denial- of-service using a GraphQL field.	https://helpx .adobe.com/s ecurity/prod ucts/magento /apsb21- 64.html	A-ADO-MAGE- 170921/86	
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 & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2021-36044		
media_encod	er				
Out-of- bounds Read	08-Sep-21	4.3 attacker could leverage this sensitive memory information in the context of		https://helpx .adobe.com/s ecurity/prod ucts/media- encoder/apsb 21-32.html	A-ADO-MEDI- 170921/87
Improper Restriction of Operations within the Bounds of a Memory Buffer	01-Sep-21	9.3	Adobe Media Encoder version 15.1 (and earlier) is affected by an improper memory access vulnerability when parsing a crafted .SVG file. An attacker could leverage this vulnerability to execute code 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-2021-36070	https://helpx .adobe.com/s ecurity/prod ucts/media- encoder/apsb 21-70.html	A-ADO-MEDI- 170921/88
medium					
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	08-Sep-21	9.3	Medium by Adobe version 2.4.5.331 (and earlier) is affected by a buffer overflow vulnerability when parsing a crafted file. An unauthenticated attacker could leverage this	https://helpx .adobe.com/s ecurity/prod ucts/medium /apsb21- 34.html	A-ADO-MEDI- 170921/89
CVSS Scoring Sc	ale 0-1	1-2	2-3 3-4 4-5 5-6 Page 31 of 1474	6-7 7-8	8-9 9-10

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			vulnerability to achieve remote 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-2021-28580		
photoshop	<u> </u>				
Out-of- bounds Write	01-Sep-21	9.3	Adobe Photoshop versions 21.2.10 (and earlier) and 22.4.3 (and earlier) are affected by a heap-based buffer overflow 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 file. CVE ID : CVE-2021-36065	https://helpx .adobe.com/s ecurity/prod ucts/photosh op/apsb21- 68.html	A-ADO-PHOT- 170921/90
Out-of- bounds Write	01-Sep-21	9.3	Adobe Photoshop versions 21.2.10 (and earlier) and 22.4.3 (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 file. CVE ID : CVE-2021-36066	https://helpx .adobe.com/s ecurity/prod ucts/photosh op/apsb21- 68.html	A-ADO-PHOT- 170921/91
xmp_toolkit_	sdk				
Stack-based Buffer	01-Sep-21	9.3	XMP Toolkit SDK version 2020.1 (and earlier) is affected by a stack-based	https://helpx .adobe.com/s ecurity/prod	A-ADO-XMP 170921/92
CVSS Scoring Sc	cale 0-1	1-2	2-3 3-4 4-5 5-6 Page 32 of 1474	6-7 7-8	8-9 9-10

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Overflow			buffer overflow vulnerability potentially resulting in arbitrary code execution in the context of the current user. Exploitation requires user interaction in that a victim must open a crafted file. CVE ID : CVE-2021-39847	ucts/xmpcore /apsb21- 65.html	
Out-of- bounds Read	01-Sep-21	4.3	XMP Toolkit SDK versions 2020.1 (and earlier) are affected by an out-of-bounds read vulnerability that could lead to disclosure of arbitrary memory. An attacker could leverage this vulnerability to bypass mitigations such as ASLR. Exploitation of this issue requires user interaction in that a victim must open a malicious file. CVE ID : CVE-2021-36045	https://helpx .adobe.com/s ecurity/prod ucts/xmpcore /apsb21- 65.html	A-ADO-XMP 170921/93
Access of Memory Location After End of Buffer	01-Sep-21	9.3	XMP Toolkit version 2020.1 (and earlier) is affected by a memory corruption vulnerability, potentially resulting in arbitrary code execution in the context of the current user. User interaction is required to exploit this vulnerability. CVE ID : CVE-2021-36046	https://helpx .adobe.com/s ecurity/prod ucts/xmpcore /apsb21- 65.html	A-ADO-XMP 170921/94
Improper Input Validation	01-Sep-21	9.3	XMP Toolkit SDK version 2020.1 (and earlier) is affected by an Improper Input Validation vulnerability potentially resulting in arbitrary code execution in	https://helpx .adobe.com/s ecurity/prod ucts/xmpcore /apsb21- 65.html	A-ADO-XMP 170921/95
Validation CVSS Scoring Sc	ale 0-1	1-2	potentially resulting in	/apsb21-	8-9 9-10

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			the context of the current user. Exploitation requires user interaction in that a victim must open a crafted file. CVE ID : CVE-2021-36047		
Improper Input Validation	01-Sep-21	9.3	XMP Toolkit SDK version 2020.1 (and earlier) is affected by an Improper Input Validation vulnerability potentially resulting in arbitrary code execution in the context of the current user. Exploitation requires user interaction in that a victim must open a crafted file. CVE ID : CVE-2021-36048	https://helpx .adobe.com/s ecurity/prod ucts/xmpcore /apsb21- 65.html	A-ADO-XMP 170921/96
Heap-based Buffer Overflow	01-Sep-21	9.3	XMP Toolkit SDK version 2020.1 (and earlier) is affected by a buffer overflow vulnerability potentially resulting in arbitrary code execution in the context of the current user. Exploitation requires user interaction in that a victim must open a crafted file. CVE ID : CVE-2021-36050	https://helpx .adobe.com/s ecurity/prod ucts/xmpcore /apsb21- 65.html	A-ADO-XMP 170921/97
Access of Memory Location After End of Buffer	01-Sep-21	6.8	XMP Toolkit version 2020.1 (and earlier) is affected by a memory corruption vulnerability, potentially resulting in arbitrary code execution in the context of the current user. User interaction is required to exploit this vulnerability.	https://helpx .adobe.com/s ecurity/prod ucts/xmpcore /apsb21- 65.html	A-ADO-XMP 170921/98

Page 34 of 1474

4.3	CVE ID : CVE-2021-36052 XMP Toolkit SDK versions 2020.1 (and earlier) are affected by an out-of-bounds read vulnerability that could lead to disclosure of arbitrary memory. An attacker could leverage this vulnerability to bypass mitigations such as ASLR. Exploitation of this issue requires user interaction in that a victim must open a malicious file.	https://helpx .adobe.com/s ecurity/prod ucts/xmpcore /apsb21- 65.html	A-ADO-XMP 170921/99
4.3	2020.1 (and earlier) are affected by an out-of-bounds read vulnerability that could lead to disclosure of arbitrary memory. An attacker could leverage this vulnerability to bypass mitigations such as ASLR. Exploitation of this issue requires user interaction in that a victim	.adobe.com/s ecurity/prod ucts/xmpcore /apsb21-	_
	CVE ID : CVE-2021-36053		
4.3	XMP Toolkit SDK version 2020.1 (and earlier) is affected by a buffer overflow vulnerability potentially resulting in local application denial of service in the context of the current user. Exploitation requires user interaction in that a victim must open a crafted file. CVE ID : CVE-2021-36054	https://helpx .adobe.com/s ecurity/prod ucts/xmpcore /apsb21- 65.html	A-ADO-XMP 170921/100
9.3	XMP Toolkit SDK versions 2020.1 (and earlier) are affected by a use-after-free 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 file. CVE ID : CVE-2021-36055	https://helpx .adobe.com/s ecurity/prod ucts/xmpcore /apsb21- 65.html	A-ADO-XMP 170921/101
9.3	XMP Toolkit SDK version 2020.1 (and earlier) is	https://helpx .adobe.com/s	A-ADO-XMP 170921/102
	9.3	 2020.1 (and earlier) is affected by a buffer overflow vulnerability potentially resulting in local application denial of service in the context of the current user. Exploitation requires user interaction in that a victim must open a crafted file. CVE ID : CVE-2021-36054 XMP Toolkit SDK versions 2020.1 (and earlier) are affected by a use-after-free 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 file. CVE ID : CVE-2021-36055 XMP Toolkit SDK version 2020.1 (and earlier) is 	 2020.1 (and earlier) is affected by a buffer overflow vulnerability potentially resulting in local application denial of service in the context of the current user. Exploitation requires user interaction in that a victim must open a crafted file. CVE ID : CVE-2021-36054 XMP Toolkit SDK versions 2020.1 (and earlier) are affected by a use-after-free 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 file. CVE ID : CVE-2021-36055 MP Toolkit SDK version XMP Toolkit SDK version AMP Toolkit SDK version

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Overflow			affected by a buffer overflow vulnerability potentially resulting in arbitrary code execution in the context of the current user. Exploitation requires user interaction in that a victim must open a crafted file. CVE ID : CVE-2021-36056	ecurity/prod ucts/xmpcore /apsb21- 65.html	
Write-what- where Condition	01-Sep-21	2.1	XMP Toolkit SDK version 2020.1 (and earlier) is affected by a write-what- where condition vulnerability caused during the application's memory allocation process. This may cause the memory management functions to become mismatched resulting in local application denial of service in the context of the current user. CVE ID : CVE-2021-36057	https://helpx .adobe.com/s ecurity/prod ucts/xmpcore /apsb21- 65.html	A-ADO-XMP 170921/103
Integer Overflow or Wraparoun d	01-Sep-21	4.3	XMP Toolkit SDK version 2020.1 (and earlier) is affected by an Integer Overflow vulnerability potentially resulting in application-level denial of service in the context of the current user. Exploitation requires user interaction in that a victim must open a crafted file. CVE ID : CVE-2021-36058	https://helpx .adobe.com/s ecurity/prod ucts/xmpcore /apsb21- 65.html	A-ADO-XMP 170921/104
Buffer Underwrite ('Buffer	01-Sep-21	9.3	XMP Toolkit version 2020.1 (and earlier) is affected by a Buffer Underflow	https://helpx .adobe.com/s ecurity/prod	A-ADO-XMP 170921/105

CVSS Scoring Scale	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10
			ſ		£ 1 / 7 /					

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			will enable calling arbitrary constructors. An attacker with access to the configuration center he will be able to poison the rule so when retrieved by the consumers, it will get RCE on all of them. This was fixed in Dubbo 2.7.13, 3.0.2 CVE ID : CVE-2021-36162		
Deserializati on of Untrusted Data	07-Sep-21	7.5	In Apache Dubbo, users may choose to use the Hessian protocol. The Hessian protocol is implemented on top of HTTP and passes the body of a POST request directly to a HessianSkeleton: New HessianSkeleton are created without any configuration of the serialization factory and therefore without applying the dubbo properties for applying allowed or blocked type lists. In addition, the generic service is always exposed and therefore attackers do not need to figure out a valid service/method name pair. This is fixed in 2.7.13, 2.6.10.1 CVE ID : CVE-2021-36163	https://lists.a pache.org/thr ead.html/r8d 0adc057bb15 a37199502cc 366f4b1164c 9c536ce28e4 defdb428c0% 40%3Cdev.du bbo.apache.or g%3E	A-APA-DUBB- 170921/108
zeppelin					
Improper Neutralizati on of Input During Web Page	02-Sep-21	4.3	Cross Site Scripting vulnerability in markdown interpreter of Apache Zeppelin allows an attacker to inject malicious scripts.	https://lists.a pache.org/thr ead.html/r90 590aa5ea788 128ecc2e822	A-APA-ZEPP- 170921/109
CVSS Scoring Sc	ale 0-1	1-2	2-3 3-4 4-5 5-6 Page 38 of 1474	6-7 7-8	8-9 9-10

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Generation ('Cross-site Scripting') Apple			This issue affects Apache Zeppelin Apache Zeppelin versions prior to 0.9.0. CVE ID : CVE-2021-27578	e1e64d5200b 4cb92b06707 b38da4cb3d %40%3Cuser s.zeppelin.ap ache.org%3E, http://www. openwall.com /lists/oss- security/202 1/09/02/3	
safari					
Improper Authenticati on	08-Sep-21	5.8	A logic issue was addressed with improved restrictions. This issue is fixed in tvOS 14.6, iOS 14.6 and iPadOS 14.6, Safari 14.1.1, macOS Big Sur 11.4, watchOS 7.5. A malicious website may be able to access restricted ports on arbitrary servers. CVE ID : CVE-2021-30720	https://supp ort.apple.com /en- us/HT21252 9, https://supp ort.apple.com /en- us/HT21252 8, https://supp ort.apple.com /en- us/HT21253 4, https://supp ort.apple.com /en- us/HT21253 2, https://supp ort.apple.com /en- us/HT21253 3	A-APP-SAFA- 170921/110
Out-of-	08-Sep-21	6.8	Multiple memory corruption	https://supp	A-APP-SAFA-

Page 39 of 1474

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
bounds Write			issues were addressed with improved memory handling. This issue is fixed in tvOS 14.6, iOS 14.6 and iPadOS 14.6, Safari 14.1.1, macOS Big Sur 11.4, watchOS 7.5. Processing maliciously crafted web content may lead to arbitrary code execution. CVE ID : CVE-2021-30734	ort.apple.com /en- us/HT21252 9, https://supp ort.apple.com /en- us/HT21252 8, https://supp ort.apple.com /en- us/HT21253 4, https://supp ort.apple.com /en- us/HT21253 2, https://supp ort.apple.com /en- us/HT21253 3,	170921/111
Access of Resource Using Incompatibl e Type ('Type Confusion')	08-Sep-21	6.8	A type confusion issue was addressed with improved state handling. This issue is fixed in iOS 14.7, Safari 14.1.2, macOS Big Sur 11.5, watchOS 7.6, tvOS 14.7. Processing maliciously crafted web content may lead to arbitrary code execution. CVE ID : CVE-2021-30758	https://supp ort.apple.com /en- us/HT21260 6, https://supp ort.apple.com /en- us/HT21260 4, https://supp ort.apple.com /en- us/HT21260 5, https://supp	A-APP-SAFA- 170921/112
CVSS Scoring Sc	ale 0-1	1-2	2-3 3-4 4-5 5-6	https://supp	8-9 9-10

3-4 4-5 5-6 Page 40 of 1474

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
N/A	08-Sep-21	6.8	This issue was addressed with improved checks. This issue is fixed in iOS 14.7, Safari 14.1.2, macOS Big Sur 11.5, watchOS 7.6, tvOS 14.7. Processing maliciously crafted web content may lead to code execution. CVE ID : CVE-2021-30797	ort.apple.com /en- us/HT21260 2, https://supp ort.apple.com /en- us/HT21260 1 https://supp ort.apple.com /en- us/HT21260 6, https://supp ort.apple.com /en- us/HT21260 4, https://supp ort.apple.com /en- us/HT21260 5, https://supp ort.apple.com /en- us/HT21260 2, https://supp ort.apple.com /en-	A-APP-SAFA- 170921/113
Arubanetwo	rks			1	
sd-wan					
Improper Neutralizati on of Special	07-Sep-21	9	A remote arbitrary command execution vulnerability was discovered in Aruba SD-WAN	https://www. arubanetwor ks.com/asset	A-ARU-SD-W- 170921/114
CVSS Scoring Sc	ale 0-1	1-2	2-3 3-4 4-5 5-6 Page 41 of 1474	6-7 7-8	8-9 9-10

Forgery (CSRF)07-Sep-215.810 8.8.0.1, 8.7.1.2, 8.8.0.6, 8.5.0.12, 8.3.0.15. Aruba has released patches for Aruba SD-WAN Software and Gateways and ArubaOS that address this security vulnerability.s/alert/ARUB A-PSA-2021- 016.txt170921/13Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')07-Sep-217.5A remote buffer overflow vulnerability was discovered in Aruba SD-WAN Software and Gateways; Aruba Operating System Software 8.6.0.8, 8.5.0.12, 8.3.0.15.https://www. arubanetwor ks.com/asset s/alert/ARUB https://www arubanetwor ks.com/asset s/alert/ARUB https://www arubanetwor ks.com/asset o16.txtA-ARU-SD- 170921/13	Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Cross-Site Request Forgery (CSRF)07-Sep-215.8forgery (csrf) vulnerability was discovered in Aruba SD- WAN Software and Gateways; Aruba Operating System Software version(s): Prior to 8.6.0.4-2.2.0.4; Prior to 8.8.0.1, 8.7.1.2, 8.6.0.8, 8.5.0.12, 8.3.0.15. Aruba has released patches for Aruba SD-WAN Software and Gateways and ArubaOS that address this security vulnerability.https://www. arubanetwor ks.com/asset s/alert/ARUB A-PSA-2021- 016.txtA-ARU-SD- I70921/11Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')07-Sep-217.5A remote buffer overflow vulnerability was discovered in Aruba SD-WAN Software and Gateways; Aruba Operating System Software version(s): Prior to 8.6.0.4- 2.2.0.4; Prior to 8.7.1.2, 8.6.0.8, 8.5.0.12, 8.3.0.15. A-ruba has released patches for Aruba SD-WAN Softwarehttps://www. arubanetwor ks.com/asset s/alert/ARUB A-ARU-SD- 170921/11	used in a Command ('Command			Aruba Operating System Software version(s): Prior to 8.6.0.4-2.2.0.4; Prior to 8.7.1.4, 8.6.0.9, 8.5.0.13, 8.3.0.16, 6.5.4.20, 6.4.4.25. Aruba has released patches for Aruba SD-WAN Software and Gateways and ArubaOS that address this security vulnerability.	A-PSA-2021-	
Buffer Copy withoutvulnerability was discovered in Aruba SD-WAN Software and Gateways; Arubahttps://www. arubanetworChecking Size of Input ('Classic Buffer Overflow')07-Sep-217.57.57.5A-ARU-SD- 2.2.0.4; Prior to 8.6.0.4- 2.2.0.4; Prior to 8.7.1.2, 8.6.0.8, 8.5.0.12, 8.3.0.15.A-ARU-SD- 3.0.15.A-ARU-SD- 170921/11	Request Forgery	07-Sep-21	5.8	forgery (csrf) vulnerability was discovered in Aruba SD- WAN Software and Gateways; Aruba Operating System Software version(s): Prior to 8.6.0.4-2.2.0.4; Prior to 8.8.0.1, 8.7.1.2, 8.6.0.8, 8.5.0.12, 8.3.0.15. Aruba has released patches for Aruba SD-WAN Software and Gateways and ArubaOS that address this security vulnerability.	arubanetwor ks.com/asset s/alert/ARUB A-PSA-2021-	A-ARU-SD-W- 170921/115
that address this security	without Checking Size of Input ('Classic Buffer	07-Sep-21	7.5	vulnerability was discovered in Aruba SD-WAN Software and Gateways; Aruba Operating System Software version(s): Prior to 8.6.0.4- 2.2.0.4; Prior to 8.7.1.2, 8.6.0.8, 8.5.0.12, 8.3.0.15. Aruba has released patches for Aruba SD-WAN Software and Gateways and ArubaOS	arubanetwor ks.com/asset s/alert/ARUB A-PSA-2021-	A-ARU-SD-W- 170921/116

Page 42 of 1474

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			vulnerability.		
			CVE ID : CVE-2021-37716		
Improper Neutralizati on of Special Elements used in a Command ('Command Injection')	07-Sep-21	9	A remote arbitrary command execution vulnerability was discovered in Aruba SD-WAN Software and Gateways; Aruba Operating System Software version(s): Prior to 8.6.0.4-2.2.0.6; Prior to 8.7.1.4, 8.6.0.7, 8.5.0.12, 8.3.0.16. Aruba has released patches for Aruba SD-WAN Software and Gateways and ArubaOS that address this security vulnerability.	https://www. arubanetwor ks.com/asset s/alert/ARUB A-PSA-2021- 016.txt	A-ARU-SD-W- 170921/117
			CVE ID : CVE-2021-37717		
Improper Neutralizati on of Special Elements used in a Command ('Command Injection')	07-Sep-21	9	A remote arbitrary command execution vulnerability was discovered in Aruba SD-WAN Software and Gateways; Aruba Operating System Software version(s): Prior to 8.6.0.4-2.2.0.6; Prior to 8.7.1.4, 8.6.0.7, 8.5.0.12, 8.3.0.16. Aruba has released patches for Aruba SD-WAN Software and Gateways and ArubaOS that address this security vulnerability. CVE ID : CVE-2021-37718	https://www. arubanetwor ks.com/asset s/alert/ARUB A-PSA-2021- 016.txt	A-ARU-SD-W- 170921/118
Improper					
Neutralizati on of Special Elements used in a Command ('Command Injection')	07-Sep-21	9	A remote arbitrary command execution vulnerability was discovered in Aruba SD-WAN Software and Gateways; Aruba Operating System Software version(s): Prior to 8.6.0.4-2.2.0.4; Prior to 8.7.1.4, 8.6.0.9, 8.5.0.13,	https://www. arubanetwor ks.com/asset s/alert/ARUB A-PSA-2021- 016.txt	A-ARU-SD-W- 170921/119
CVSS Scoring Sc	ale 0-1	1-2	2-3 3-4 4-5 5-6	6-7 7-8	8-9 9-10

Page 43 of 1474

			8.3.0.16, 6.5.4.20, 6.4.4.25. Aruba has released patches for Aruba SD-WAN Software and Gateways and ArubaOS that address this security vulnerability.		
			CVE ID : CVE-2021-37719		
Improper Neutralizati on of Special Elements used in a Command ('Command Injection')	07-Sep-21	9	A remote arbitrary command execution vulnerability was discovered in Aruba SD-WAN Software and Gateways; Aruba Operating System Software version(s): Prior to 8.6.0.4-2.2.0.4; Prior to 8.7.1.4, 8.6.0.9, 8.5.0.13, 8.3.0.16, 6.5.4.20, 6.4.4.25. Aruba has released patches for Aruba SD-WAN Software and Gateways and ArubaOS that address this security vulnerability. CVE ID : CVE-2021-37720	https://www. arubanetwor ks.com/asset s/alert/ARUB A-PSA-2021- 016.txt	A-ARU-SD-W- 170921/120
Improper Neutralizati on of Special Elements used in a Command ('Command Injection')	07-Sep-21	9	A remote arbitrary command execution vulnerability was discovered in Aruba SD-WAN Software and Gateways; Aruba Operating System Software version(s): Prior to 8.6.0.4-2.2.0.4; Prior to 8.7.1.4, 8.6.0.9, 8.5.0.13, 8.3.0.16, 6.5.4.20, 6.4.4.25. Aruba has released patches for Aruba SD-WAN Software and Gateways and ArubaOS that address this security vulnerability. CVE ID : CVE-2021-37721	https://www. arubanetwor ks.com/asset s/alert/ARUB A-PSA-2021- 016.txt	A-ARU-SD-W- 170921/121
Atlassian					
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			
atlasboard								
Improper Limitation of a Pathname to a Restricted Directory ('Path Traversal')	01-Sep-21	5	The renderWidgetResource resource in Atlasian Atlasboard before version 1.1.9 allows remote attackers to read arbitrary files via a path traversal vulnerability. CVE ID : CVE-2021-39109	https://bitbu cket.org/atlas sian/atlasboa rd/commits/ 9c03df09f09 399e260101 0466e8ba3a2 8236eb9c	A-ATL-ATLA- 170921/122			
data_center								
Improper Control of Generation of Code ('Code Injection')	01-Sep-21	9	Affected versions of Atlassian Jira Service Management Server and Data Center allow remote attackers with "Jira Administrators" access to execute arbitrary Java code or run arbitrary system commands via a Server_Side Template Injection vulnerability in the Email Template feature. The affected versions are before version 4.13.9, and from version 4.14.0 before 4.18.0.	N/A	A-ATL-DATA- 170921/123			
N/A	08-Sep-21	4.3	Affected versions of Atlassian Jira Server and Data Center allow remote attackers to impact the application's availability via a Denial of Service (DoS) vulnerability in the GIF Image Reader component. The affected versions are before version 8.19.0. CVE ID : CVE-2021-39116	https://jira.at lassian.com/b rowse/JRASE RVER-72738	A-ATL-DATA- 170921/124			
Improper Authenticati	01-Sep-21	5	Affected versions of Atlassian Jira Server and Data Center	N/A	A-ATL-DATA- 170921/125			
CVSS Scoring Sc	ale 0-1	1-2	2-3 3-4 4-5 5-6 Page 45 of 1474	6-7 7-8	8-9 9-10			

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
on			allow users who have watched an issue to continue receiving updates on the issue even after their Jira account is revoked, via a Broken Access Control vulnerability in the issue notification feature. The affected versions are before version 8.19.0. CVE ID : CVE-2021-39119		
N/A	08-Sep-21	4	Affected versions of Atlassian Jira Server and Data Center allow authenticated remote attackers to enumerate the keys of private Jira projects via an Information Disclosure vulnerability in the /rest/api/latest/projectvalid ate/key endpoint. The affected versions are before version 8.5.18, from version 8.6.0 before 8.13.10, and from version 8.14.0 before 8.18.2. CVE ID : CVE-2021-39121	https://jira.at lassian.com/b rowse/JRASE RVER-72715	A-ATL-DATA- 170921/126
N/A	08-Sep-21	5	Affected versions of Atlassian Jira Server and Data Center allow anonymous remote attackers to view users' emails via an Information Disclosure vulnerability in the /rest/api/2/search endpoint. The affected versions are before version 8.5.13, from version 8.6.0 before 8.13.5, and from version 8.14.0 before 8.15.1.	https://jira.at lassian.com/b rowse/JRASE RVER-72293	A-ATL-DATA- 170921/127

CVSS Scoring Scale	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10
			F	Page 46 o	f 1474					

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2021-39122		
jira					
N/A	08-Sep-21	4.3	Affected versions of Atlassian Jira Server and Data Center allow remote attackers to impact the application's availability via a Denial of Service (DoS) vulnerability in the GIF Image Reader component. The affected versions are before version 8.19.0.	https://jira.at lassian.com/b rowse/JRASE RVER-72738	A-ATL-JIRA- 170921/128
			CVE ID : CVE-2021-39116		
Improper Authenticati on	01-Sep-21	5	Affected versions of Atlassian Jira Server and Data Center allow users who have watched an issue to continue receiving updates on the issue even after their Jira account is revoked, via a Broken Access Control vulnerability in the issue notification feature. The affected versions are before version 8.19.0. CVE ID : CVE-2021-39119	N/A	A-ATL-JIRA- 170921/129
N/A	08-Sep-21	4	Affected versions of Atlassian Jira Server and Data Center allow authenticated remote attackers to enumerate the keys of private Jira projects via an Information Disclosure vulnerability in the /rest/api/latest/projectvalid ate/key endpoint. The affected versions are before version 8.5.18, from version 8.6.0 before 8.13.10, and	https://jira.at lassian.com/b rowse/JRASE RVER-72715	A-ATL-JIRA- 170921/130

CVSS Scoring Scale	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9
			P	Page 47 of	f 1474				

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			from version 8.14.0 before 8.18.2.		
			CVE ID : CVE-2021-39121		
N/A	08-Sep-21	5	Affected versions of Atlassian Jira Server and Data Center allow anonymous remote attackers to view users' emails via an Information Disclosure vulnerability in the /rest/api/2/search endpoint. The affected versions are before version 8.5.13, from version 8.6.0 before 8.13.5, and from version 8.14.0 before 8.15.1.	https://jira.at lassian.com/b rowse/JRASE RVER-72293	A-ATL-JIRA- 170921/131
			CVE ID : CVE-2021-39122		
jira_service_	management				
Improper Control of Generation of Code ('Code Injection')	01-Sep-21	9	Affected versions of Atlassian Jira Service Management Server and Data Center allow remote attackers with "Jira Administrators" access to execute arbitrary Java code or run arbitrary system commands via a Server_Side Template Injection vulnerability in the Email Template feature. The affected versions are before version 4.13.9, and from version 4.14.0 before 4.18.0. CVE ID : CVE-2021-39115	N/A	A-ATL-JIRA- 170921/132
Barco					
mirrorop_wi	ndows_sende	er			
Improper Control of Generation	07-Sep-21	7.2	Barco MirrorOp Windows Sender before 2.5.3.65 uses cleartext HTTP and thus	https://www. barco.com/en /support/cm	A-BAR-MIRR- 170921/133
CVSS Scoring Sc	cale 0-1	1-2	2-3 3-4 4-5 5-6	6-7 7-8	8-9 9-10

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
of Code ('Code Injection')			allows rogue software upgrades. An attacker on the local network can achieve remote code execution on any computer that tries to update Windows Sender due to the fact that the upgrade mechanism is not secured (is not protected with TLS). CVE ID : CVE-2021-38142	s, https://www. barco.com/en /support/soft ware/R3305 0099?majorV ersion=2&mi norVersion=5 &patchVersio n=3&buildVe rsion=65	
better_error: better_error:					
Cross-Site Request Forgery (CSRF)	07-Sep-21	6.8	better_errors is an open source replacement for the standard Rails error page with more information rich error pages. It is also usable outside of Rails in any Rack app as Rack middleware. better_errors prior to 2.8.0 did not implement CSRF protection for its internal requests. It also did not enforce the correct "Content- Type" header for these requests, which allowed a cross-origin "simple request" to be made without CORS protection. These together left an application with better_errors enabled open to cross-origin attacks. As a developer tool, better_errors documentation strongly recommends addition only to the `development` bundle group, so this vulnerability should only affect	https://githu b.com/Better Errors/better _errors/com mit/8e8e796 bfbde4aa088 741823c8a3f c6df2089bb0, https://githu b.com/Better Errors/better _errors/secur ity/advisorie s/GHSA- w3j4-76qw- wwjm, https://githu b.com/Better Errors/better _errors/better _errors/better _errors/better _474	A-BET-BETT- 170921/134

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

			development environments. Please ensure that your project limits better_errors to		
			the `development` group (or the non-Rails equivalent). Starting with release 2.8.x, CSRF protection is enforced. It is recommended that you upgrade to the latest release, or minimally to "~> 2.8.3". There are no known workarounds to mitigate the risk of using older releases of better_errors. CVE ID : CVE-2021-39197		
bookstackap	0				
bookstack	P				
Server-Side Request Forgery (SSRF)	02-Sep-21	4	bookstack is vulnerable to Server-Side Request Forgery (SSRF) CVE ID : CVE-2021-3758	https://githu b.com/bookst ackapp/book stack/commit /bee5e2c7ca 637d034c698 5c0328cef0ce 068778e, https://huntr .dev/bounties /a8d7fb24- 9a69-42f3- 990a- 2db93b53f76 b	A-BOO-BOOK- 170921/135
Improper Neutralizati on of Input During Web Page Generation ('Cross-site	06-Sep-21	3.5	bookstack is vulnerable to Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') CVE ID : CVE-2021-3767	https://huntr .dev/bounties /7ec92c85- 30eb-4071- 8891- 6183446ca98 0,	A-BOO-BOOK- 170921/136

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Scripting')				https://githu b.com/bookst ackapp/book stack/commit /040997fdc4 414776bcac0 6a3cbaac3b2 6b5e8a64	
Improper Neutralizati on of Input During Web Page Generation ('Cross-site Scripting')	06-Sep-21	3.5	bookstack is vulnerable to Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') CVE ID : CVE-2021-3768	https://githu b.com/bookst ackapp/book stack/commit /5e6092aaf8f d420202016 0382865548 60bf8ea64, https://huntr .dev/bounties /64a0229f- ff5e-4c64- b83e- 9bfc0698a78 e	A-BOO-BOOK- 170921/137
botan_projec	:t				
botan					
Use of a Broken or Risky Cryptograph ic Algorithm	06-Sep-21	2.6	The ElGamal implementation in Botan through 2.18.1, as used in Thunderbird and other products, allows plaintext recovery because, during interaction between two cryptographic libraries, a certain dangerous combination of the prime defined by the receiver's public key, the generator defined by the receiver's public key, and the sender's ephemeral exponents can	https://githu b.com/rando mbit/botan/p ull/2790	A-BOT-BOTA- 170921/138
CVSS Scoring Sc	ale 0-1	1-2	2-3 3-4 4-5 5-6	6-7 7-8	8-9 9-10

Page 51 of 1474

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			lead to a cross-configuration attack against OpenPGP.		
			CVE ID : CVE-2021-40529		
cashtomer_p	roiect				
cashtomer					
Improper Neutralizati on of Special Elements used in an SQL Command ('SQL Injection')	06-Sep-21	6.5	An editid GET parameter of the Cashtomer WordPress plugin through 1.0.0 is not properly sanitised, escaped or validated before inserting to a SQL statement, leading to SQL injection. CVE ID : CVE-2021-24391	N/A	A-CAS-CASH- 170921/139
Cisco	<u> </u>			<u> </u>	
enterprise_n	fv_infrastruc	ture_so	oftware		
Improper Authenticati on	02-Sep-21	9.3	A vulnerability in the TACACS+ authentication, authorization and accounting (AAA) feature of Cisco Enterprise NFV Infrastructure Software (NFVIS) could allow an unauthenticated, remote attacker to bypass authentication and log in to an affected device as an administrator. This vulnerability is due to incomplete validation of user-supplied input that is passed to an authentication script. An attacker could exploit this vulnerability by injecting parameters into an authentication request. A successful exploit could allow the attacker to bypass	https://tools. cisco.com/sec urity/center/ content/Cisco SecurityAdvis ory/cisco-sa- nfvis- g2DMVVh	A-CIS-ENTE- 170921/140

Page 52 of 1474

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			authentication and log in as an administrator to the affected device.		
			CVE ID : CVE-2021-34746		
evolved_prog	grammable_n	etworl	k_manager		
Insufficientl y Protected Credentials	02-Sep-21	2.1	A vulnerability in the CLI of Cisco Prime Infrastructure and Cisco Evolved Programmable Network (EPN) Manager could allow an authenticated, local attacker to access sensitive information stored on the underlying file system of an affected system. This vulnerability exists because sensitive information is not sufficiently secured when it is stored. An attacker could exploit this vulnerability by gaining unauthorized access to sensitive information on an affected system. A successful exploit could allow the attacker to create forged authentication requests and gain unauthorized access to the affected system.	https://tools. cisco.com/sec urity/center/ content/Cisco SecurityAdvis ory/cisco-sa- prime-info- disc-nTU9FJ2	A-CIS-EVOL- 170921/141
			CVE ID : CVE-2021-34733		
identity_serv	vices_engine			1	
Improper Neutralizati on of Input During Web Page Generation ('Cross-site Scripting')	02-Sep-21	3.5	A vulnerability in the web- based management interface of Cisco Identity Services Engine (ISE) Software could allow an authenticated, remote attacker with administrative credentials to conduct a cross-site scripting	https://tools. cisco.com/sec urity/center/ content/Cisco SecurityAdvis ory/cisco-sa- ise-xss- 4HnZFewr	A-CIS-IDEN- 170921/142
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 & CVE ID	Patch	NCIIPC ID
			(XSS) attack against a user of the interface. This vulnerability exists because the web-based management interface does not properly validate user-supplied input. An attacker could exploit this vulnerability by injecting malicious code into specific pages of the interface. A successful exploit could allow the attacker to execute arbitrary script code in the context of the interface or access sensitive, browser- based information. To exploit this vulnerability, an attacker would need valid administrative credentials.		
nexus_insigh	its				
Files or Directories Accessible to External Parties	02-Sep-21	4	A vulnerability in the web UI for Cisco Nexus Insights could allow an authenticated, remote attacker to view and download files related to the web application. The attacker requires valid device credentials. This vulnerability exists because proper role-based access control (RBAC) filters are not applied to file download actions. An attacker could exploit this vulnerability by logging in to the application and then navigating to the directory listing and download functions. A	https://tools. cisco.com/sec urity/center/ content/Cisco SecurityAdvis ory/cisco-sa- insight- infodis- 2By2ZpBB	A-CIS-NEXU- 170921/143

CVSS Scoring Scale	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10
Dago 54 of 1474										

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			successful exploit could allow the attacker to download sensitive files that should be restricted, which could result in disclosure of sensitive information.		
			CVE ID : CVE-2021-34765		
prime_collab	oration_prov	risionin	ıg		
Improper Neutralizati on of Input During Web Page Generation ('Cross-site Scripting')	02-Sep-21	4.3	A vulnerability in the web- based management interface of Cisco Prime Collaboration Provisioning could allow an unauthenticated, remote attacker to conduct a cross- site scripting (XSS) attack against a user of the interface. This vulnerability is due to insufficient validation of user-supplied input by the web-based management interface. An attacker could exploit this vulnerability by persuading a user of the interface to click a crafted link. A successful exploit could allow the attacker to execute arbitrary script code in the context of the interface or access sensitive, browser-based information. CVE ID : CVE-2021-34732	https://tools. cisco.com/sec urity/center/ content/Cisco SecurityAdvis ory/cisco-sa- prime-collab- xss- fQMDE5GO	A-CIS-PRIM- 170921/144
prime_infras	tructure				
Insufficientl y Protected Credentials	02-Sep-21	2.1	A vulnerability in the CLI of Cisco Prime Infrastructure and Cisco Evolved Programmable Network (EPN) Manager could allow	https://tools. cisco.com/sec urity/center/ content/Cisco SecurityAdvis	A-CIS-PRIM- 170921/145

CVSS Scoring Scale	0-1	1-2	2-3	3-4	4-5	5-6			

7-8

6-7

8-9

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			an authenticated, local attacker to access sensitive information stored on the underlying file system of an affected system. This vulnerability exists because sensitive information is not sufficiently secured when it is stored. An attacker could exploit this vulnerability by gaining unauthorized access to sensitive information on an affected system. A successful exploit could allow the attacker to create forged authentication requests and gain unauthorized access to the affected system.	ory/cisco-sa- prime-info- disc-nTU9FJ2	
cliniccases	<u> </u>				
cliniccases					
Improper Neutralizati on of Input During Web Page Generation ('Cross-site Scripting')	07-Sep-21	4.3	Multiple reflected cross-site scripting (XSS) vulnerabilities in ClinicCases 7.3.3 allow unauthenticated attackers to introduce arbitrary JavaScript by crafting a malicious URL. This can result in account takeover via session token theft.	N/A	A-CLI-CLIN- 170921/146
Cross-Site Request Forgery (CSRF)	07-Sep-21	6.8	CVE ID : CVE-2021-38704 ClinicCases 7.3.3 is affected by Cross-Site Request Forgery (CSRF). A successful attack would consist of an authenticated user following a malicious link, resulting in	N/A	A-CLI-CLIN- 170921/147

CVSS Scoring Scale	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8
			Г		F 1 / 7 /			

8-9

Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
		arbitrary actions being carried out with the privilege level of the targeted user. This can be exploited to create a secondary administrator account for the attacker.		
07-Sep-21	6.5	messages_load.php in ClinicCases 7.3.3 suffers from a blind SQL injection vulnerability, which allows low-privileged attackers to execute arbitrary SQL commands through a vulnerable parameter. CVE ID : CVE-2021-38706	https://clinic cases.com	A-CLI-CLIN- 170921/148
07-Sep-21	3.5	Persistent cross-site scripting (XSS) vulnerabilities in ClinicCases 7.3.3 allow low- privileged attackers to introduce arbitrary JavaScript to account parameters. The XSS payloads will execute in the browser of any user who views the relevant content. This can result in account takeover via session token theft. CVE ID : CVE-2021-38707	N/A	A-CLI-CLIN- 170921/149
<u> </u>	ject			
ghlighter				
06-Sep-21	6.5	A c GET parameter of the Comment Highlighter WordPress plugin through 0.13 is not properly sanitised,	N/A	A-COM- COMM- 170921/150
	07-Sep-21 07-Sep-21 07-Sep-21	07-Sep-21 6.5 07-Sep-21 3.5 Shlighter_project Shlighter_project	07-Sep-21A a.5arbitrary actions being carried out with the privilege level of the targeted user. This can be exploited to create a secondary administrator account for the attacker.07-Sep-216.5messages_load.php in ClinicCases 7.3.3 suffers from a blind SQL injection vulnerability, which allows low-privileged attackers to execute arbitrary SQL commands through a vulnerable parameter.07-Sep-218.5Persistent cross-site scripting (XSS) vulnerabilities in ClinicCases 7.3.3 allow low- privileged attackers to introduce arbitrary JavaScript to account parameters. The XSS payloads will execute in the browser of any user who views the relevant content. This can result in account takeover via session token theft. CVE ID : CVE-2021-3870706-Sep-216.5A c GET parameter of the Comment Highlighter WordPress plugin through	or.arbitrary actions being carried out with the privilege level of the targeted user. This can be exploited to create a secondary administrator account for the attacker.arbitrary actions being carried out with the privilege level of the targeted user. This can be exploited to create a secondary administrator account for the attacker.arbitrary actions being carried out with the privileged level of the targeted user. This can be exploited to create a secondary administrator account for the attacker.arbitrary count of the attacker.07-Sep-216.5messages_load.php in ClinicCases 7.3.3 suffers from a blind SQL injection vulnerability, which allows low-privileged attackers to

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
SQL Command ('SQL Injection')			inserting to a SQL statement, leading to SQL injection. CVE ID : CVE-2021-24393		
cozyvision					
sms_alert_or	der_notificati	ons			
Improper Neutralizati on of Input During Web Page Generation ('Cross-site Scripting')	06-Sep-21	4.3	The SMS Alert Order Notifications WordPress plugin before 3.4.7 is affected by a cross site scripting (XSS) vulnerability in the plugin's setting page. CVE ID : CVE-2021-24588	N/A	A-COZ-SMS 170921/151
Cryptopp					
crypto\\+\\+	F				
Use of a Broken or Risky Cryptograph ic Algorithm	06-Sep-21	2.6	The ElGamal implementation in Crypto++ through 8.5 allows plaintext recovery because, during interaction between two cryptographic libraries, a certain dangerous combination of the prime defined by the receiver's public key, the generator defined by the receiver's public key, and the sender's ephemeral exponents can lead to a cross-configuration attack against OpenPGP. CVE ID : CVE-2021-40530	N/A	A-CRY-CRYP- 170921/152
cyberark credential_provider					
Inadequate Encryption Strength	02-Sep-21	5	An inadequate encryption vulnerability discovered in CyberArk Credential Provider before 12.1 may	N/A	A-CYB-CRED- 170921/153
CVSS Scoring Sc	ale 0-1	1-2	2-3 3-4 4-5 5-6 Page 58 of 1474	6-7 7-8	3 <u>8-9</u> <u>9-10</u>

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			lead to Information Disclosure. An attacker may realistically have enough information that the number of possible keys (for a credential file) is only one, and the number is usually not higher than 2^36. CVE ID : CVE-2021-31796		
Concurrent Execution using Shared Resource with Improper Synchroniza tion ('Race Condition')	02-Sep-21	1.9	The user identification mechanism used by CyberArk Credential Provider prior to 12.1 is susceptible to a local host race condition, leading to password disclosure. CVE ID : CVE-2021-31797	N/A	A-CYB-CRED- 170921/154
Inadequate Encryption Strength	02-Sep-21	1.9	The effective key space used to encrypt the cache in CyberArk Credential Provider prior to 12.1 has low entropy, and under certain conditions a local malicious user can obtain the plaintext of cache files. CVE ID : CVE-2021-31798	N/A	A-CYB-CRED- 170921/155
identity					
Improper Authenticati on	01-Sep-21	5	CyberArk Identity 21.5.131, when handling an invalid authentication attempt, sometimes reveals whether the username is valid. In certain authentication policy configurations with MFA, the API response length can be used to differentiate between	https://www. cyberark.com /products/	A-CYB-IDEN- 170921/156

CVSS Scoring Scale	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10
			F	Page 59 of	f 1474					

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			a valid user and an invalid one (aka Username Enumeration). Response differentiation enables attackers to enumerate usernames of valid application users. Attackers can use this information to leverage brute-force and dictionary attacks in order to discover valid account information such as passwords.		
			CVE ID : CVE-2021-37151		
Cybernetikz					
easy_social_i	cons				
Improper Neutralizati on of Input During Web Page Generation ('Cross-site Scripting')	02-Sep-21	4.3	The Easy Social Icons plugin <= 3.0.8 for WordPress echoes out the raw value of `\$_SERVER['PHP_SELF']` in its main file. On certain configurations including Apache+modPHP this makes it possible to use it to perform a reflected Cross- Site Scripting attack by injecting malicious code in the request path. CVE ID : CVE-2021-39322	N/A	A-CYB-EASY- 170921/157
Cyrus					
imap					
Use of a Broken or Risky Cryptograph ic Algorithm	01-Sep-21	5	Cyrus IMAP before 3.4.2 allows remote attackers to cause a denial of service (multiple-minute daemon hang) via input that is mishandled during hash- table interaction. Because	https://www. cyrusimap.or g/imap/dow nload/release - notes/index.h tml,	A-CYR-IMAP- 170921/158

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			there are many insertions into a single bucket, strcmp becomes slow. This is fixed in 3.4.2, 3.2.8, and 3.0.16. CVE ID : CVE-2021-33582	https://githu b.com/cyrusi map/cyrus- imapd/comm its/master, https://cyrus .topicbox.com /groups/ann ounce/T3dde 0a23524629 75- M1386fc44ad f967e072f8df 13/cyrus- imap-3-4-2- 3-2-8-and-3- 0-16-released	
Deskpro					
deskpro					
Improper Neutralizati on of Input During Web Page Generation ('Cross-site Scripting')	08-Sep-21	3.5	Deskpro cloud and on- premise Deskpro 2021.1.6 and fixed in Deskpro 2021.1.7 contains a cross-site scripting (XSS) vulnerability in the download file feature on a manager profile due to lack of input validation. CVE ID : CVE-2021-36695	N/A	A-DES-DESK- 170921/159
Improper Neutralizati on of Input During Web Page Generation ('Cross-site Scripting')	07-Sep-21	3.5	Deskpro cloud and on- premise Deskpro 2021.1.6 and fixed in Deskpro 2021.1.7 contains a cross-site scripting (XSS) vulnerability in social media links on a user profile due to lack of input validation. CVE ID : CVE-2021-36696	N/A	A-DES-DESK- 170921/160
dna88					
CVSS Scoring Sc	ale 0-1	1-2	2-3 3-4 4-5 5-6 Page 61 of 1474	6-7 7-8	8-9 9-10

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
highlight				I	I
Improper Neutralizati on of Input During Web Page Generation ('Cross-site Scripting')	06-Sep-21	3.5	The Highlight WordPress plugin before 0.9.3 does not sanitise its CustomCSS setting, allowing high privilege users to perform Cross-Site Scripting attacks even when the unfiltered_html capability is disallowed	N/A	A-DNA-HIGH- 170921/161
			CVE ID : CVE-2021-24591		
easy_testimo	nial_manage	r_proje	ect		
easy_testimo	nial_manage	r			
Improper Neutralizati on of Special Elements used in an SQL Command ('SQL Injection')	06-Sep-21	6.5	An id GET parameter of the Easy Testimonial Manager WordPress plugin through 1.2.0 is not sanitised, escaped or validated before inserting to a SQL statement, leading to SQL injection CVE ID : CVE-2021-24394	N/A	A-EAS-EASY- 170921/162
Eclipse					
theia					
Exposure of Resource to Wrong Sphere	01-Sep-21	6.8	In Eclipse Theia 0.3.9 to 1.8.1, the "mini-browser" extension allows a user to preview HTML files in an iframe inside the IDE. But with the way it is made it is possible for a previewed HTML file to trigger an RCE. This exploit only happens if a user previews a malicious file CVE ID : CVE-2021-34435	https://bugs. eclipse.org/b ugs/show_bu g.cgi?id=5680 18	A-ECL-THEI- 170921/163
Improper Limitation CVSS Scoring Sc	02-Sep-21	7.5	In Eclipse Theia 0.1.1 to 0.2.0, it is possible to exploit the 2-3 3-4 4-5 5-6	https://bugs. eclipse.org/b	A-ECL-THEI- 170921/164 8-9 9-10

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
of a Pathname to a Restricted Directory ('Path Traversal')			default build to obtain remote code execution (and XXE) via the theia-xml- extension. This extension uses lsp4xml (recently renamed to LemMinX) in order to provide language support for XML. This is installed by default. CVE ID : CVE-2021-34436	ugs/show_bu g.cgi?id=5631 74	
eigentech					
natural_lang	uage_process	ing			
Incorrect Authorizatio n	07-Sep-21	5.5	In Eigen NLP 3.10.1, a lack of access control on the /auth/v1/sso/config/ SSO configuration endpoint allows any logged-in user (guest, standard, or admin) to view and modify information. CVE ID : CVE-2021-38615	https://eigen tech.com/	A-EIG-NATU- 170921/165
Incorrect Authorizatio n	07-Sep-21	6.5	In Eigen NLP 3.10.1, a lack of access control on the /auth/v1/user/{user-guid}/ user edition endpoint could permit any logged-in user to increase their own permissions via a user_permissions array in a PATCH request. A guest user could modify other users' profiles and much more. CVE ID : CVE-2021-38616	https://eigen tech.com/	A-EIG-NATU- 170921/166
Incorrect Authorizatio n CVSS Scoring Sc	07-Sep-21	6.5	In Eigen NLP 3.10.1, a lack of access control on the /auth/v1/user/ user creation endpoint allows a standard user to create a	https://eigen tech.com/	A-EIG-NATU- 170921/167 8-9 9-10

Page 63 of 1474

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			super user account with a defined password. This directly leads to privilege escalation.		
			CVE ID : CVE-2021-38617		
elfinder.netc	ore_project				
elfinder.netc	ore				
Improper Input Validation	01-Sep-21	7.5	This affects all versions of package elFinder.NetCore. The ExtractAsync function within the FileSystem is vulnerable to arbitrary extraction due to insufficient validation.	N/A	A-ELF-ELFI- 170921/168
			CVE ID : CVE-2021-23427		
Improper Input Validation	01-Sep-21	7.5	This affects all versions of package elFinder.NetCore. The Path.Combine() method is used to create an absolute file path. Due to missing sanitation of the user input and a missing check of the generated path its possible to escape the Files directory via path traversal CVE ID : CVE-2021-23428	N/A	A-ELF-ELFI- 170921/169
espressif	L			L	
esp-idf					
Improper Input Validation	07-Sep-21	3.3	The Bluetooth Classic implementation in Espressif ESP-IDF 4.4 and earlier does not properly handle the reception of continuous unsolicited LMP responses, allowing attackers in radio range to trigger a denial of service (crash) in ESP32 by	N/A	A-ESP-ESP 170921/170
CVSS Scoring Sc	ale 0-1	1-2	2-3 3-4 4-5 5-6 Page 64 of 1474	6-7 7-8	8-9 9-10

Page 64 of 1474

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			flooding the target device with LMP Feature Response data. CVE ID : CVE-2021-28135		
Out-of- bounds Write	07-Sep-21	3.3	The Bluetooth Classic implementation in Espressif ESP-IDF 4.4 and earlier does not properly handle the reception of multiple LMP IO Capability Request packets during the pairing process, allowing attackers in radio range to trigger memory corruption (and consequently a crash) in ESP32 via a replayed (duplicated) LMP packet.	https://www. espressif.com /en/products /socs/esp32	A-ESP-ESP 170921/171
N/A	07-Sep-21	8.3	CVE ID : CVE-2021-28136 The Bluetooth Classic implementation in Espressif ESP-IDF 4.4 and earlier does not properly restrict the Feature Page upon reception of an LMP Feature Response Extended packet, allowing attackers in radio range to trigger arbitrary code execution in ESP32 via a crafted Extended Features bitfield payload. CVE ID : CVE-2021-28139	https://www. espressif.com /en/products /socs/esp32	A-ESP-ESP 170921/172
eyoucms					
eyoucms					
Improper Neutralizati on of Input During Web Page	07-Sep-21	3.5	Eyoucms 1.5.4 lacks sanitization of input data, allowing an attacker to inject malicious code into `filename` param to trigger	N/A	A-EYO-EYOU- 170921/173
CVSS Scoring Sc	ale 0-1	1-2	2-3 3-4 4-5 5-6 Page 65 of 1474	6-7 7-8	8-9 9-10

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Generation ('Cross-site Scripting')			Reflected XSS. CVE ID : CVE-2021-39496		
Server-Side Request Forgery (SSRF)	07-Sep-21	7.5	eyoucms 1.5.4 lacks sanitization of input data, allowing an attacker to inject a url to trigger blind SSRF via the saveRemote() function. CVE ID : CVE-2021-39497	N/A	A-EYO-EYOU- 170921/174
Improper Neutralizati on of Input During Web Page Generation ('Cross-site Scripting')	07-Sep-21	4.3	A Cross-site scripting (XSS) vulnerability in Users in Qiong ICP EyouCMS 1.5.4 allows remote attackers to inject arbitrary web script or HTML via the `title` parameter in bind_email function. CVE ID : CVE-2021-39499	N/A	A-EYO-EYOU- 170921/175
URL Redirection to Untrusted Site ('Open Redirect')	07-Sep-21	5.8	EyouCMS 1.5.4 is vulnerable to Open Redirect. An attacker can redirect a user to a malicious url via the Logout function. CVE ID : CVE-2021-39501	N/A	A-EYO-EYOU- 170921/176
F-secure	I			I	I
atlant					
Loop with Unreachable Exit Condition ('Infinite Loop')	chable tion ite07-Sep-214.3scanning WIM archive file can lead to denial-of-service (infinite loop and freezes AV engine scanner). The uulnerability can be exploit		https://www. f- secure.com/e n/business/p rograms/vuln erability- reward- program/hall -of-fame, https://www. f-	A-F-S-ATLA- 170921/177	

CVSS Scoring Scale	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10
Page 66 of 1474										

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
cloud_protec	tion_for_sale	sforce	Anti-Virus engine. CVE ID : CVE-2021-33599	secure.com/e n/business/s upport-and- downloads/s ecurity- advisories/cv e-2021- 33599 https://www.	
Loop with Unreachable Exit Condition ('Infinite Loop')	07-Sep-21	4.3	A vulnerability affecting F- Secure Antivirus engine was discovered whereby scanning WIM archive file can lead to denial-of-service (infinite loop and freezes AV engine scanner). The vulnerability can be exploit remotely by an attacker. A successful attack will result in Denial-of-Service of the Anti-Virus engine. CVE ID : CVE-2021-33599	f- secure.com/e n/business/p rograms/vuln erability- reward- program/hall -of-fame, https://www. f- secure.com/e n/business/s upport-and- downloads/s ecurity- advisories/cv e-2021- 33599	A-F-S-CLOU- 170921/178
elements_en	dpoint_prote	ction			
Loop with Unreachable Exit Condition ('Infinite Loop')		A vulnerability affecting F- Secure Antivirus engine was discovered whereby scanning WIM archive file can lead to denial-of-service (infinite loop and freezes AV engine scanner). The vulnerability can be exploit remotely by an attacker. A successful attack will result	https://www. f- secure.com/e n/business/p rograms/vuln erability- reward- program/hall -of-fame, https://www.	A-F-S-ELEM- 170921/179	

Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID				
		in Denial-of-Service of the Anti-Virus engine. CVE ID : CVE-2021-33599	f- secure.com/e n/business/s upport-and- downloads/s ecurity- advisories/cv e-2021- 33599					
ty			<u>.</u>	<u> </u>				
07-Sep-21	4.3	A vulnerability affecting F- Secure Antivirus engine was discovered whereby scanning WIM archive file can lead to denial-of-service (infinite loop and freezes AV engine scanner). The vulnerability can be exploit remotely by an attacker. A successful attack will result in Denial-of-Service of the Anti-Virus engine. CVE ID : CVE-2021-33599	https://www. f- secure.com/e n/business/p rograms/vuln erability- reward- program/hall -of-fame, https://www. f- secure.com/e n/business/s upport-and- downloads/s ecurity- advisories/cv e-2021- 33599	A-F-S-LINU- 170921/180				
file-upload-with-preview_project								
viui-preview			https://githu					
05-Sep-21	4.3	This affects the package file- upload-with-preview before 4.2.0. A file containing malicious JavaScript code in the name can be uploaded (a user needs to be tricked into uploading such a file).	https://githu b.com/johnda tserakis/file- upload-with- preview/pull /40/files?file- filters%5B% 5D=.js&hide-	A-FIL-FILE- 170921/181				
	vith-preview_vith-preview	v v v v v	orbitin Denial-of-Service of the Anti-Virus engine. CVE ID : CVE-2021-33599cvCVE ID : CVE-2021-33599cvA vulnerability affecting F- Secure Antivirus engine was discovered whereby scanning WIM archive file can lead to denial-of-service (infinite loop and freezes AV engine scanner). The vulnerability can be exploit remotely by an attacker. A successful attack will result in Denial-of-Service of the Anti-Virus engine. CVE ID : CVE-2021-33599vith-preview_projectvith-preview05-Sep-214.34.3This affects the package file- upload-with-preview before 4.2.0. A file containing malicious JavaScript code in the name can be uploaded (a user needs to be tricked into uploading such a file).	of - Service of the Anti-Virus engine. CVE ID : CVE-2021-33599f- secure.com/e n/business/s upport-and- downloads/s ecurity- advisories/cv e-2021- 33599yyA vulnerability affecting F- Secure Antivirus engine was discovered whereby scanning WIM archive file can lead to denial-of-service (infinite loop and freezes AV engine scanner). The vulnerability can be exploit remotely by an attacker. A successful attack will result in Denial-of-Service of the Anti-Virus engine. CVE ID : CVE-2021-33599https://www. f- secure.com/e n/business/p rograms/vuln erability- reward- program/hall -of-fame, https://www. f- secure.com/e n/business/s upport-and- downloads/s ecurity- advisories/cv e-2021- 3359907-Sep-214.3This affects the package file- upload-with-preview before 4.2.0. A file containing malicious JavaSript code in the name can be uploaded (a user needs to be tricked into uploading such a file).https://githu b.com/johnda tserakis/file- tile-sysB% SD=js&hide-				

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Scripting')			CVE ID : CVE-2021-23439	deleted- files=true%2 3diff- fe47b243de1 7419c0daa22 cd785cd754b aed60cf3679 d3da1d6fe00 6f9f4a7f0R17 4	
Fortinet					
fortimanager	ſ				
Incorrect Authorizatio n	06-Sep-21	6.5	An improper access control vulnerability in FortiManager versions 6.4.0 to 6.4.3 may allow an authenticated attacker with a restricted user profile to access the SD- WAN Orchestrator panel via directly visiting its URL. CVE ID : CVE-2021-24006	https://fortig uard.com/ad visory/FG-IR- 20-061	A-FOR-FORT- 170921/182
fortiweb					
Out-of- bounds Write	08-Sep-21	6.5	A stack-based buffer overflow in Fortinet FortiWeb version 6.3.14 and below, 6.2.4 and below allows attacker to execute unauthorized code or commands via crafted parameters in CLI command execution	https://fortig uard.com/ad visory/FG-IR- 20-206	A-FOR-FORT- 170921/183
Improper Neutralizati on of Special Elements used in an OS CVSS Scoring Sc	08-Sep-21 ale 0-1	6.5	CVE ID : CVE-2021-36179A Improper neutralization of special elements used in a command ('Command Injection') in Fortinet FortiWeb version 6.3.13 and below allows attacker to2-33-44-55-6	https://fortig uard.com/ad visory/FG-IR- 21-047 6-7 7-8	A-FOR-FORT- 170921/184 8-9 9-10

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID							
Command ('OS Command		execute unauthorized code or commands via crafted HTTP requests										
Injection')			CVE ID : CVE-2021-36182									
frentix												
openolat												
XML Injection (aka Blind XPath Injection)	01-Sep-21	6.5	OpenOlat is a web-based learning management system (LMS). Prior to version 15.3.18, 15.5.3, and 16.0.0, using a prepared import XML file (e.g. a course) any class on the Java classpath can be instantiated, including spring AOP bean factories. This can be used to execute code arbitrary code by the attacker. The attack requires an OpenOlat user account with the authoring role. It can not be exploited by unregistered users. The problem is fixed in versions 15.3.18, 15.5.3, and 16.0.0. There are no known workarounds aside from upgrading. CVE ID : CVE-2021-39181	https://githu b.com/OpenO LAT/OpenOL AT/commit/ 3f219ac457af de82e3be57b c614352ab92 c05684, https://githu b.com/OpenO LAT/OpenOL AT/security/ advisories/G HSA-596v- 3gwh-2m9w	A-FRE-OPEN- 170921/185							
gambit	words											
titan_framew			The iframe-font-preview.php									
ImproperNeutralization of InputDuring WebPageGeneration('Cross-site		4.3	file of the titan-framework does not properly escape the font-weight and font-family GET parameters before outputting them back in an href attribute, leading to Reflected Cross-Site Scripting	N/A	A-GAM-TITA- 170921/186							
('Cross-site CVSS Scoring Sc	cale 0-1	1-2	-	6-7 7-8	8-9 9-10							

Page 70 of 1474

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Scripting')			issues		
			CVE ID : CVE-2021-24435		
gdprinfo					
cookie_notic	e_\\&_conser	ıt_banı	ner_for_gdpr_\\&_ccpa_compli	ance	
Improper Neutralizati on of Input During Web Page Generation ('Cross-site Scripting')	06-Sep-21	3.5	The Cookie Notice & Consent Banner for GDPR & CCPA Compliance WordPress plugin before 1.7.2 does not properly sanitize inputs to prevent injection of arbitrary HTML within the plugin's design customization options. CVE ID : CVE-2021-24590	N/A	A-GDP-COOK- 170921/187
geekwebsolı	Ition				
embed_yout					
Improper Neutralizati on of Special Elements used in an SQL Command ('SQL	06-Sep-21	6.5	The editid GET parameter of the Embed Youtube Video WordPress plugin through 1.0 is not sanitised, escaped or validated before inserting to a SQL statement, leading to SQL injection. CVE ID : CVE-2021-24395	N/A	A-GEE-EMBE- 170921/188
Injection') geminilabs					
site_reviews					
Improper Neutralizati on of Input During Web Page Generation ('Cross-site Scripting')	06-Sep-21	3.5	The Site Reviews WordPress plugin before 5.13.1 does not sanitise some of its Review Details when adding a review as an admin, which could allow them to perform Cross- Site Scripting attacks when the unfiltered_html is disallowed	N/A	A-GEM-SITE- 170921/189

CVSS Scoring Scale	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10
Page 71 of 1474										

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2021-24603		
ghost					
ghost					
Improper Privilege Managemen t	03-Sep-21	6.5	Ghost is a Node.js content management system. An error in the implementation of the limits service between versions 4.0.0 and 4.9.4 allows all authenticated users (including contributors) to view admin-level API keys via the integrations API endpoint, leading to a privilege escalation vulnerability. This issue is patched in Ghost version 4.10.0. As a workaround, disable all non-Administrator accounts to prevent API access. It is highly recommended to regenerate all API keys after patching or applying the workaround. CVE ID : CVE-2021-39192	https://githu b.com/TryGh ost/Ghost/se curity/adviso ries/GHSA- j5c2-hm46- wp5c	A-GHO-GHOS- 170921/190
gibbonedu					
gibbon					
Improper Neutralizati on of Input During Web Page Generation ('Cross-site Scripting')	03-Sep-21	4.3	A reflected XSS vulnerability exists in multiple pages in version 22 of the Gibbon application that allows for arbitrary execution of JavaScript (gibbonCourseClassID, gibbonPersonID, subpage, currentDate, or allStudents to index.php). CVE ID : CVE-2021-40492	https://gibbo nedu.org/	A-GIB-GIBB- 170921/191

 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
GNU				<u> </u>	
inetutils					
Insufficient Verification of Data Authenticity	03-Sep-21	4.3	The ftp client in GNU Inetutils before 2.2 does not validate addresses returned by PASV/LSPV responses to make sure they match the server address. This is similar to CVE-2020-8284 for curl. CVE ID : CVE-2021-40491	https://git.sa vannah.gnu.o rg/cgit/inetut ils.git/commi t/?id=58cb04 3b190fd04eff daea7c94034 16b436e50d d, https://lists.g nu.org/archiv e/html/bug- inetutils/202 1- 06/msg0000 2.html	A-GNU-INET- 170921/192
Gnupg					
libgcrypt					
Use of a Broken or Risky Cryptograph ic Algorithm	06-Sep-21	2.6	The ElGamal implementation in Libgcrypt before 1.9.4 allows plaintext recovery because, during interaction between two cryptographic libraries, a certain dangerous combination of the prime defined by the receiver's public key, the generator defined by the receiver's public key, and the sender's ephemeral exponents can lead to a cross-configuration attack against OpenPGP. CVE ID : CVE-2021-40528	N/A	A-GNU-LIBG- 170921/193
Google	<u> </u>			l	
chrome					
CVSS Scoring Sc	ale 0-1	1-2	2-3 3-4 4-5 5-6	6-7 7-8	8-9 9-10

Page 73 of 1474

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Use After Free	03-Sep-21	6.8	Use after free in Blink in Google Chrome prior to 93.0.4577.63 allowed an attacker who convinced a user to drag and drop a malicous folder to a page to potentially perform a sandbox escape via a crafted HTML page. CVE ID : CVE-2021-30606	https://chro mereleases.g oogleblog.co m/2021/08/ stable- channel- update-for- desktop_31.ht ml	A-GOO-CHRO- 170921/194
Use After Free	03-Sep-21	6.8	Use after free in Permissions in Google Chrome prior to 93.0.4577.63 allowed a remote attacker who had compromised the renderer process to potentially exploit heap corruption via a crafted HTML page. CVE ID : CVE-2021-30607	https://chro mereleases.g oogleblog.co m/2021/08/ stable- channel- update-for- desktop_31.ht ml	A-GOO-CHRO- 170921/195
Use After Free	03-Sep-21	6.8	Use after free in Web Share in Google Chrome prior to 93.0.4577.63 allowed a remote attacker to potentially exploit heap corruption via a crafted HTML page. CVE ID : CVE-2021-30608	https://chro mereleases.g oogleblog.co m/2021/08/ stable- channel- update-for- desktop_31.ht ml	A-GOO-CHRO- 170921/196
Use After Free	03-Sep-21	6.8	Use after free in Sign-In in Google Chrome prior to 93.0.4577.63 allowed a remote attacker to potentially exploit heap corruption via a crafted HTML page. CVE ID : CVE-2021-30609	https://chro mereleases.g oogleblog.co m/2021/08/ stable- channel- update-for- desktop_31.ht ml	A-GOO-CHRO- 170921/197
Use After	03-Sep-21	6.8	Use after free in Extensions	https://chro	A-GOO-CHRO-
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 & CVE ID	Patch	NCIIPC ID
Free			API in Google Chrome prior to 93.0.4577.63 allowed a remote attacker to potentially exploit heap corruption via a crafted HTML page. CVE ID : CVE-2021-30610	mereleases.g oogleblog.co m/2021/08/ stable- channel- update-for- desktop_31.ht ml	170921/198
Use After Free	03-Sep-21	6.8	Use after free in WebRTC in Google Chrome on Linux, ChromeOS prior to 93.0.4577.63 allowed an attacker who convinced a user to install a malicious extension to potentially exploit heap corruption via a crafted HTML page. CVE ID : CVE-2021-30611	https://chro mereleases.g oogleblog.co m/2021/08/ stable- channel- update-for- desktop_31.ht ml	A-GOO-CHRO- 170921/199
Use After Free	03-Sep-21	6.8	Use after free in WebRTC in Google Chrome on Linux, ChromeOS prior to 93.0.4577.63 allowed an attacker who convinced a user to install a malicious extension to potentially exploit heap corruption via a crafted HTML page. CVE ID : CVE-2021-30612	https://chro mereleases.g oogleblog.co m/2021/08/ stable- channel- update-for- desktop_31.ht ml	A-GOO-CHRO- 170921/200
Use After Free	03-Sep-21	6.8	Use after free in Base internals in Google Chrome prior to 93.0.4577.63 allowed a remote attacker to potentially exploit heap corruption via a crafted HTML page. CVE ID : CVE-2021-30613	https://chro mereleases.g oogleblog.co m/2021/08/ stable- channel- update-for- desktop_31.ht ml	A-GOO-CHRO- 170921/201
Out-of-	03-Sep-21	6.8	Heap buffer overflow in	https://chro	A-GOO-CHRO-
CVSS Scoring Sc	ale 0-1	1-2	2-3 3-4 4-5 5-6	6-7 7-8	8-9 9-10

Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
		TabStrip in Google Chrome prior to 93.0.4577.63 allowed an attacker who convinced a user to install a malicious extension to potentially exploit heap corruption via a crafted HTML page.	mereleases.g oogleblog.co m/2021/08/ stable- channel- update-for- desktop_31.ht ml	170921/202
03-Sep-21	4.3	Inappropriate implementation in Navigation in Google Chrome prior to 93.0.4577.63 allowed a remote attacker to leak cross-origin data via a crafted HTML page. CVE ID : CVE-2021-30615	https://chro mereleases.g oogleblog.co m/2021/08/ stable- channel- update-for- desktop_31.ht ml	A-GOO-CHRO- 170921/203
03-Sep-21	6.8	Use after free in Media in Google Chrome prior to 93.0.4577.63 allowed a remote attacker to potentially exploit heap corruption via a crafted HTML page. CVE ID : CVE-2021-30616	https://chro mereleases.g oogleblog.co m/2021/08/ stable- channel- update-for- desktop_31.ht ml	A-GOO-CHRO- 170921/204
03-Sep-21	4.3	Policy bypass in Blink in Google Chrome prior to 93.0.4577.63 allowed a remote attacker to bypass site isolation via a crafted HTML page. CVE ID : CVE-2021-30617	https://chro mereleases.g oogleblog.co m/2021/08/ stable- channel- update-for- desktop_31.ht ml	A-GOO-CHRO- 170921/205
03-Sep-21	6.8	Inappropriate implementation in DevTools in Google Chrome prior to	https://chro mereleases.g oogleblog.co	A-GOO-CHRO- 170921/206
	03-Sep-21 03-Sep-21	- -	Image: Constraint of the series of the ser	Image: Note of the section of the s

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			93.0.4577.63 allowed a remote attacker who had convinced the user to use Chrome headless with remote debugging to execute arbitrary code via a crafted HTML page. CVE ID : CVE-2021-30618	m/2021/08/ stable- channel- update-for- desktop_31.ht ml	
Authenticati on Bypass by Spoofing	03-Sep-21	4.3	Inappropriate implementation in Autofill in Google Chrome prior to 93.0.4577.63 allowed a remote attacker to spoof security UI via a crafted HTML page. CVE ID : CVE-2021-30619	https://chro mereleases.g oogleblog.co m/2021/08/ stable- channel- update-for- desktop_31.ht ml	A-GOO-CHRO- 170921/207
N/A	03-Sep-21	6.8	Insufficient policy enforcement in Blink in Google Chrome prior to 93.0.4577.63 allowed a remote attacker to bypass content security policy via a crafted HTML page. CVE ID : CVE-2021-30620	https://chro mereleases.g oogleblog.co m/2021/08/ stable- channel- update-for- desktop_31.ht ml	A-GOO-CHRO- 170921/208
Authenticati on Bypass by Spoofing	03-Sep-21	4.3	Inappropriate implementation in Autofill in Google Chrome prior to 93.0.4577.63 allowed a remote attacker to spoof security UI via a crafted HTML page. CVE ID : CVE-2021-30621	https://chro mereleases.g oogleblog.co m/2021/08/ stable- channel- update-for- desktop_31.ht ml	A-GOO-CHRO- 170921/209
Use After Free CVSS Scoring Sca	03-Sep-21	6.8	Use after free in WebApp Installs in Google Chrome prior to 93.0.4577.63 allowed an attacker who 2-3 3-4 4-5 5-6	https://chro mereleases.g oogleblog.co m/2021/08/	A-GOO-CHRO- 170921/210 8-9 9-10

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			convinced a user to install a malicious extension to potentially exploit heap corruption via a crafted HTML page. CVE ID : CVE-2021-30622	stable- channel- update-for- desktop_31.ht ml	
Use After Free	03-Sep-21	6.8	Use after free in Bookmarks in Google Chrome prior to 93.0.4577.63 allowed an attacker who convinced a user to install a malicious extension to potentially exploit heap corruption via a crafted HTML page. CVE ID : CVE-2021-30623	https://chro mereleases.g oogleblog.co m/2021/08/ stable- channel- update-for- desktop_31.ht ml	A-GOO-CHRO- 170921/211
Use After Free	03-Sep-21	6.8	Use after free in Autofill in Google Chrome prior to 93.0.4577.63 allowed a remote attacker to potentially exploit heap corruption via a crafted HTML page. CVE ID : CVE-2021-30624	https://chro mereleases.g oogleblog.co m/2021/08/ stable- channel- update-for- desktop_31.ht ml	A-GOO-CHRO- 170921/212
Haproxy	I			I	
haproxy					
Integer Overflow or Wraparoun d	08-Sep-21	5	An integer overflow exists in HAProxy 2.0 through 2.5 in htx_add_header that can be exploited to perform an HTTP request smuggling attack, allowing an attacker to bypass all configured http- request HAProxy ACLs and possibly other ACLs. CVE ID : CVE-2021-40346	https://git.ha proxy.org/?p =haproxy.git, https://githu b.com/hapro xy/haproxy/c ommit/3b69 886f7dcc3cfb 3d16630901 8e6cfec9ce2c 95	A-HAP-HAPR- 170921/213

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			
hashicorp	hashicorp							
consul								
Improper Certificate Validation	07-Sep-21	6.5	HashiCorp Consul and Consul Enterprise 1.10.1 Raft RPC layer allows non-server agents with a valid certificate signed by the same CA to access server-only functionality, enabling privilege escalation. Fixed in 1.8.15, 1.9.9 and 1.10.2. CVE ID : CVE-2021-37219	https://discu ss.hashicorp.c om/t/hcsec- 2021-22- consul-raft- rpc-privilege- escalation/29 024, https://www. hashicorp.co m/blog/categ ory/consul	A-HAS-CONS- 170921/214			
nomad								
Improper Certificate Validation	07-Sep-21	6.5	HashiCorp Nomad and Nomad Enterprise Raft RPC layer allows non-server agents with a valid certificate signed by the same CA to access server-only functionality, enabling privilege escalation. Fixed in 1.0.10 and 1.1.4. CVE ID : CVE-2021-37218	https://discu ss.hashicorp.c om/t/hcsec- 2021-21- nomad-raft- rpc-privilege- escalation/29 023, https://www. hashicorp.co m/blog/categ ory/nomad	A-HAS-NOMA- 170921/215			
IBM								
planning_ana	alytics							
N/A	01-Sep-21	4	IBM Planning Analytics 2.0 could allow a remote attacker to obtain sensitive information when a stack trace is returned in the browser. IBM X-Force ID: 205527. CVE ID : CVE-2021-29851	https://www. ibm.com/sup port/pages/n ode/6480413 , https://excha nge.xforce.ib mcloud.com/ vulnerabilitie	A-IBM-PLAN- 170921/216			
CVSS Scoring Sc	ale 0-1	1-2	2-3 3-4 4-5 5-6	6-7 7-8	8-9 9-10			

Neutralizati on of Input During Web Page Generation ('Cross-site Scripting')01-Sep-21allows 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: 205528.nge.xforce.ib mcloud.com/ vulnerabilitie s/205528, https://www. ibm.com/sup port/pages/n ode/6480413A-IBM-PLAN A-IBM-PLAN 170921/217Very potentially leading to credentials disclosure within a trusted session. IBM X- Force ID: 205528.ibm.com/sup port/pages/n ode/6480413A-IBM-PLAN A-IBM-PLAN 170921/217IBM Planning Analytics 2.0 could expose informationhttps://excha nge.xforce.ibhttps://excha nge.xforce.ib	Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Improper Neutralizati on of Input During Web Page Generation ('Cross-site Scripting')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: 205528.https://excha nge.xforce.ib https://www. ibm.com/sup port/pages/n ode/6480413A-IBM-PLAN A-IBM-PLAN 170921/217LLLIBM Planning Analytics 2.0 could expose informationhttps://excha nge.xforce.ibA-IBM-PLAN potentially leading to credentials disclosure within a trusted session. IBM X- force ID: 205528.Https://excha nge.xforce.ibA-IBM-PLAN potentially leading to credentials disclosure within a trusted session. IBM X- force ID: 205528.					s/205527	
IBM Planning Analytics 2.0 https://excha could expose information nge.xforce.ib	Improper Neutralizati on of Input During Web Page Generation ('Cross-site Scripting')	01-Sep-21	3.5	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: 205528.	nge.xforce.ib mcloud.com/ vulnerabilitie s/205528, https://www. ibm.com/sup port/pages/n	A-IBM-PLAN- 170921/217
could expose information nge.xforce.ib				LVE ID : LVE-2021-29852		
Unchecked Return 01-Sep-21 4 validating the return values s/205529, 170921/218	Unchecked Return Value	01-Sep-21	4	could expose information that could be used to to create attacks by not validating the return values from some methods or functions. IBM X-Force ID: 205529.	nge.xforce.ib mcloud.com/ vulnerabilitie s/205529, https://www. ibm.com/sup port/pages/n	A-IBM-PLAN- 170921/218
mmer_project	immer_proje	ct				L
mmer	immer					
Resource Using Incompatibl e Type01-Sep-217.528477 when the user- provided keys used in the path parameter are arrays. In particular, this bypass is possible because the condition (n === " prote " 1540542SNPM- 1579266, https://snyk.i 0/vuln/SNYKA-IMM-IMM 170921/219	Access of Resource Using Incompatibl e Type ('Type Confusion')	01-Sep-21	7.5	<pre>immer before 9.0.6. A type confusion vulnerability can lead to a bypass of CVE-2020- 28477 when the user- provided keys used in the path parameter are arrays. In particular, this bypass is possible because the condition (p === "_proto_" p === "constructor") in applyPatches_ returns false if p is ['_proto_'] (or</pre>	o/vuln/SNYK -JAVA- ORGWEBJAR SNPM- 1579266, https://snyk.i o/vuln/SNYK -JS-IMMER- 1540542, https://githu b.com/immer js/immer/co	A-IMM-IMME- 170921/219
CVSS Scoring Scale 0-1 1-2 2-3 3-4 4-5 5-6 6-7 7-8 8-9 9-10	CVSS Scoring Sc		1_2	7-3 3-1 1 -5 5.6	6-7 7-8	8-9 9-10

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			operator (strict equality operator) returns false if the operands have different type. CVE ID : CVE-2021-23436	55ee9bd42ae 08cc239102b 665a239582 37	
Improperly Controlled Modification of Dynamically -Determined Object Attributes	02-Sep-21	7.5	immer is vulnerable to Improperly Controlled Modification of Object Prototype Attributes ('Prototype Pollution') CVE ID : CVE-2021-3757	https://huntr .dev/bounties /23d38099- 71cd-42ed- a77a- 71e68094adf a, https://githu b.com/immer js/immer/co mmit/fa671e 55ee9bd42ae 08cc239102b 665a239582 37	A-IMM-IMME- 170921/220
ivanti workspace_c	ontrol				
N/A	01-Sep-21	4.6	An issue was discovered in Ivanti Workspace Control before 10.6.30.0. A locally authenticated user with low privileges can bypass File and Folder Security by leveraging an unspecified attack vector. As a result, the attacker can start applications with elevated privileges. CVE ID : CVE-2021-36235	https://foru ms.ivanti.com /s/article/A- locally- authenticated -user-with- low- privileges- can-bypass- the-File-and- Folder- Security-by- leveraging- an- unspecified- attack-vector	A-IVA-WORK- 170921/221
Jforum					
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 & CVE ID	Patch	NCIIPC ID
jforum					
Improper Neutralizati on of Input During Web Page Generation ('Cross-site Scripting')	04-Sep-21	3.5	ViewCommon.java in JForum2 2.7.0 allows XSS via a user signature. CVE ID : CVE-2021-40509	https://sourc eforge.net/p/ jforum2/code /934/	A-JFO-JFOR- 170921/222
jiangqie					
official_webs	ite_mini_pro	gram			
Improper Neutralizati on of Special Elements used in an SQL Command ('SQL Injection')	06-Sep-21	6.5	The JiangQie Official Website Mini Program WordPress plugin before 1.1.1 does not escape or validate the id GET parameter before using it in SQL statements, leading to SQL injection issues CVE ID : CVE-2021-24303	N/A	A-JIA-OFFI- 170921/223
kaml_project	t		<u> </u>		<u> </u>
kaml					
Loop with Unreachable Exit Condition ('Infinite Loop')	07-Sep-21	4	kaml is an open source implementation of the YAML format with support for kotlinx.serialization. In affected versions attackers that could provide arbitrary YAML input to an application that uses kaml could cause the application to endlessly loop while parsing the input. This could result in resource starvation and denial of service. This only affects applications that use polymorphic serialization with the default tagged	https://githu b.com/charle skorn/kaml/i ssues/179, https://githu b.com/charle skorn/kaml/c ommit/e187 85d043fc632 4c81e968aae 9764b4b060 bc6a, https://githu b.com/charle skorn/kaml/s ecurity/advis	A-KAM- KAML- 170921/224
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 & CVE ID	Patch	NCIIPC ID			
			polymorphism style. Applications using the property polymorphism style are not affected. YAML input for a polymorphic type that provided a tag but no value for the object would trigger the issue. Version 0.35.3 or later contain the fix for this issue. CVE ID : CVE-2021-39194	ories/GHSA- fmm9-3gv8- 58f4				
Kaseya	Kaseya							
unitrends_ba	ckup_softwa	re						
Improper Privilege Managemen t	01-Sep-21	9	An issue was discovered in the server software in Kaseya Unitrends Backup Software before 10.5.5-2. There is a privilege escalation from read-only user to admin. CVE ID : CVE-2021-40385	N/A	A-KAS-UNIT- 170921/225			
N/A	01-Sep-21	9	An issue was discovered in the server software in Kaseya Unitrends Backup Software before 10.5.5-2. There is authenticated remote code execution. CVE ID : CVE-2021-40387	N/A	A-KAS-UNIT- 170921/226			
keyword_me	ta_project							
keyword_me	ta							
Cross-Site Request Forgery (CSRF)	06-Sep-21	3.5	The Keyword Meta WordPress plugin through 3.0 does not sanitise of escape its settings before outputting them back in the page after they are saved, allowing for Cross-Site Scripting issues.	N/A	A-KEY-KEYW- 170921/227			
CVSS Scoring Sc	ale 0-1	1-2	2-3 3-4 4-5 5-6 Page 83 of 1474	6-7 7-8	8-9 9-10			

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Furthermore, it is also lacking any CSRF check, allowing attacker to make a logged in high privilege user save arbitrary setting via a CSRF attack.		
			CVE ID : CVE-2021-24611		
Kubernetes					
kubernetes			[.		
Incorrect Authorizatio n	URL Redirection to Untrusted Site ('Open Redirect') Hand Constant denies Hat could allow neurophysics (affected by this vui if they run a Validation Admission Webhook Nodes that denies based at least part old state of the No Validating Admiss Webhook does not some previous fiel CVE ID : CVE-202 A security issue with discovered in Kub where a user may redirect pod traffic networks on a Noo Kubernetes alread creation of Endpoi the localhost or lin range, but the sam		A security issue was discovered in kube-apiserver that could allow node updates to bypass a Validating Admission Webhook. Clusters are only affected by this vulnerability if they run a Validating Admission Webhook for Nodes that denies admission based at least partially on the old state of the Node object. Validating Admission Webhook does not observe some previous fields.	https://githu b.com/kuber netes/kubern etes/issues/1 00096	A-KUB-KUBE- 170921/228
URL Redirection to Untrusted Site ('Open Redirect')			CVE ID : CVE-2021-25735 A security issue was discovered in Kubernetes where a user may be able to redirect pod traffic to private networks on a Node. Kubernetes already prevents creation of Endpoint IPs in the localhost or link-local range, but the same validation was not performed	https://githu b.com/kuber netes/kubern etes/issues/1 02106	A-KUB-KUBE- 170921/229
			on EndpointSlice IPs. CVE ID : CVE-2021-25737		

CVSS Scoring Scale	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10	
Page 84 of 1474											

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
librenms		<u> </u>		L	
librenms					
Improper Neutralizati on of Input During Web Page Generation ('Cross-site Scripting')	08-Sep-21	3.5	In LibreNMS < 21.3.0, a stored XSS vulnerability was identified in the API Access page due to insufficient sanitization of the \$api- >description variable. As a result, arbitrary Javascript code can get executed. CVE ID : CVE-2021-31274	https://com munity.libren ms.org/t/vul nerability- report-cross- site-scripting- xss-in-the- api-access- page/15431, https://githu b.com/libren ms/librenms /pull/12739	A-LIB-LIBR- 170921/230
Magento					
magento					
Exposure of Sensitive Information to an Unauthorize d Actor	08-Sep-21	4	Magento versions 2.4.2 (and earlier), 2.4.1-p1 (and earlier) and 2.3.6-p1 (and earlier) are vulnerable to an Information Disclosure vulnerability when uploading a modified png file to a product image. Successful exploitation could lead to the disclosure of document root path by an unauthenticated attacker. Access to the admin console is required for successful exploitation. CVE ID : CVE-2021-28566	https://helpx .adobe.com/s ecurity/prod ucts/magento /apsb21- 30.html	A-MAG- MAGE- 170921/231
Incorrect Authorizatio n	uthorizatio 08-Sep-21 4		Magento versions 2.4.2 (and earlier), 2.4.1-p1 (and earlier) and 2.3.6-p1 (and earlier) are vulnerable to an Improper Authorization vulnerability in the	https://helpx .adobe.com/s ecurity/prod ucts/magento /apsb21- 30.html	A-MAG- MAGE- 170921/232

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			customers module. Successful exploitation could allow a low-privileged user to modify customer data. Access to the admin console is required for successful exploitation.		
Microfocus			CVE ID : CVE-2021-28567		
	<u>gor</u>				
Exposure of Resource to Wrong Sphere	Exposure of Resource to Wrong Sphere 02-Sep-21 2.1 pc 02-Sep-21 5.0		This release addresses a potential information leakage vulnerability in NetIQ Access Manager versions prior to 5.0.1 CVE ID : CVE-2021-22525	https://supp ort.microfocu s.com/kb/do c.php?id=702 5254	A-MIC-ACCE- 170921/233
network_aut	omation				L
uRLRedirectionto UntrustedSite ('OpenRedirect')		5.8	Open Redirect vulnerability in Micro Focus Network Automation, affecting Network Automation versions 10.4x, 10.5x, 2018.05, 2018.11, 2019.05, 2020.02, 2020.08, 2020.11, 2021.05. The vulnerability could allow redirect users to malicious websites after authentication. CVE ID : CVE-2021-38123	https://porta l.microfocus.c om/s/article/ KM00000167 3	A-MIC-NETW- 170921/234
Microsoft					
edge					
N/A	02-Sep-21	4	Microsoft Edge for Android Spoofing Vulnerability CVE ID : CVE-2021-38641	https://porta l.msrc.micros oft.com/en- US/security- guidance/adv isory/CVE-	A-MIC-EDGE- 170921/235
CVSS Scoring Sc	ale 0-1	1-2	2-3 3-4 4-5 5-6 Page 86 of 1474	6-7 7-8	8-9 9-10

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
				2021-38641	
N/A	02-Sep-21 4		Microsoft Edge for iOS Spoofing Vulnerability CVE ID : CVE-2021-38642	https://porta l.msrc.micros oft.com/en- US/security- guidance/adv isory/CVE- 2021-38642	A-MIC-EDGE- 170921/236
Improper Privilege Managemen t	02-Sep-21	6.8	Microsoft Edge (Chromium- based) Elevation of Privilege Vulnerability This CVE ID is unique from CVE-2021- 36930. CVE ID : CVE-2021-26436	https://porta l.msrc.micros oft.com/en- US/security- guidance/adv isory/CVE- 2021-26436	A-MIC-EDGE- 170921/237
N/A	02-Sep-21	4.3	Microsoft Edge for Android Information Disclosure Vulnerability CVE ID : CVE-2021-26439	https://porta l.msrc.micros oft.com/en- US/security- guidance/adv isory/CVE- 2021-26439	A-MIC-EDGE- 170921/238
Improper Privilege Managemen t	02-Sep-21	6.8	Microsoft Edge (Chromium- based) Elevation of Privilege Vulnerability This CVE ID is unique from CVE-2021- 26436. CVE ID : CVE-2021-36930	https://porta l.msrc.micros oft.com/en- US/security- guidance/adv isory/CVE- 2021-36930	A-MIC-EDGE- 170921/239
miraheze					
globalnewfile	es				
Improper Input Validation	01-Sep-21	4.3	GlobalNewFiles is a MediaWiki extension maintained by Miraheze. Prior to commit number cee254e1b158cdb0ddbea71 6b1d3edc31fa4fb5d, the username column of the	https://githu b.com/mirah eze/GlobalNe wFiles/securi ty/advisories /GHSA-57p5- hqjq-h7vg,	A-MIR-GLOB- 170921/240
CVSS Scoring Sca	ale 0-1	1-2	2-3 3-4 4-5 5-6 Page 87 of 1474	6-7 7-8	8-9 9-10

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			GlobalNewFiles special page is vulnerable to a stored XSS. Commit number cee254e1b158cdb0ddbea71 6b1d3edc31fa4fb5d contains a patch. As a workaround, one may disallow <,> (or other characters required to insert html/js) from being used in account names so an XSS is not possible. CVE ID : CVE-2021-39186	https://githu b.com/mirah eze/GlobalNe wFiles/comm it/cee254e1b 158cdb0ddbe a716b1d3edc 31fa4fb5d	
misskey					
misskey					
Server-Side Request Forgery (SSRF)	07-Sep-21	4	Misskey is an open source, decentralized microblogging platform. In affected versions a Server-Side Request Forgery vulnerability exists in "Upload from URL" and remote attachment handling. This could result in the disclosure of non-public information within the internal network. This has been fixed in 12.90.0. However, if you are using a proxy, you will need to take additional measures. As a workaround this exploit may be avoided by appropriately restricting access to private networks from the host where the application is running. CVE ID : CVE-2021-39195	https://githu b.com/missk ey- dev/misskey /security/adv isories/GHSA -mqv7-gxh4- r5vf, https://githu b.com/missk ey- dev/misskey /commit/e1a 8b158e04ad5 67d92d8daf3 cc0898ee18f 1a2e	A-MIS-MISS- 170921/241
mpath_proje	ect				
mpath					
CVSS Scoring Se	cale 0-1	1-2	2-3 3-4 4-5 5-6 Page 88 of 1474	6-7 7-8	8-9 9-10

Access of Resource Using Incompatible of Type ConfusionThis affects the package mpath before 0.8.4. A type confusion vulnerability can lead to a bypass of CVE-2018- 16490. In particular, the condition igmoreProperties indexOf(par ts[i]) !== -1 returns -1 if parts[j] Is[_proto_]. This is because the method that has because the method that has because the method that has been called if the input is an array is Array.prototype.indexOf(). They behave differently depending on the type of the input. CVE ID : CVE-2021-23438https://githu b.com/aheck mam/mpath /commit/894 02d2880d4ea 3518480a8c9 847c54112d8 24fcA-MPA-MPAT- 170921/242mrdocmrdoc is vulnerable to Deserializati on of Untrusted Datahttps://githu b.com/anitse r2016/mrdoc /commit/bb4 9e1287700b 4c76103821c a/2d282064ca a3518480a8c9 847c54112d8 24fcA-MRD- MRD- 170921/242 170921/243mrdocmrdoc is vulnerable to Deserialization of Untrusted Data CVE ID : CVE-2021-32568https://githu b.com/zmister r2016/mrdoc /commit/bb4 9e1287700b 4c76103821c a/2d2 2d21-4cad- a090- e403cd66b5a dA-MRD- MRD- 170921/243myfwctttttttmyfwcttttttttttttorus04tttttttttttorus04tttttttttttorus04ttttttt<	Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID				
nrdoc Beserializati on of Untrusted Data 06-Sep-21 06-Sep-21 06-Sep-21 06-Sep-21 06-Sep-21 07 07 07 07 07 07 07 07 07 07 07 07 07	Resource Using Incompatibl e Type ('Type	cess of source ing compatibl01-Sep-217.5mpath before confusion vulu lead to a bypath 16490. In part condition ignorePropert ts[i])!== -1 re parts[i] is ['] because the million been called if to 		mpath before 0.8.4. A type confusion vulnerability can lead to a bypass of CVE-2018- 16490. In particular, the condition ignoreProperties.indexOf(par ts[i]) !== -1 returns -1 if parts[i] is ['_proto_']. This is because the method that has been called if the input is an array is Array.prototype.indexOf() and not String.prototype.indexOf(). They behave differently depending on the type of the input.	b.com/aheck mann/mpath /commit/894 02d2880d4ea 3518480a8c9 847c541f2d8	A-MPA-MPAT- 170921/242				
Deserializati on of Untrusted DataNetps://githu b.com/zmiste (2016/mrdoc) 427016/mrdoc 42681eab54) 4661093821c 0ataA-MRD- 02187700b 467681eab54) 467681eab54 170921/243 170921/243 170921/243 170921/243 104fc04b3- 2dc1-4cad- a090- 2dc1-4cad- 	mrdoc	<u> </u>			<u> </u>					
Deserializati on of Untrusted Data6.8mrdoc is vulnerable to Deserialization of Untrusted Datab.com/zmiste r2016/mrdoc /commit/bb4 9e1287700b 4e7681eab54 4c61093821c e72f6, https://huntr .dev/bounties /04fc04b3- 2dc1-4cad- a090- e403cd66b5a dA-MRD- MRDo- 170921/243myfwcmrdoc is vulnerable to Deserialization of Untrusted DataA-MRD- e72f6, https://huntr .dev/bounties /04fc04b3- 2dc1-4cad- a090- e403cd66b5a d	mrdoc									
fish_\\ _hunt_fl	on of Untrusted	06-Sep-21	6.8	Deserialization of Untrusted Data	b.com/zmiste r2016/mrdoc /commit/bb4 9e1287700b 4e7681eab54 4c61093821c e72f6, https://huntr .dev/bounties /04fc04b3- 2dc1-4cad- a090- e403cd66b5a	MRDO-				
	myfwc									
CVSS Scoring Scale 0-1 1-2 2-3 3-4 4-5 5-6 6-7 7-8 8-9 9-10	fish_\\ _hunt_fl									
Page 89 of 1474	CVSS Scoring Sc	ale 0-1	1-2		6-7 7-8	8-9 9-10				

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Incorrect Authorizatio n	08-Sep-21	attacker to retrieve other people's personal information and images of their hunting/fishing licenses. CVE ID : CVE-2021-33981		N/A	A-MYF-FISH- 170921/244
Insufficient Session Expiration	An insufficient session expiration vulnerability exists in the "Fish Hun iOS app version 3.8.0 a earlier, which allows a remote attacker to reus spoof, or steal other us admin sessions.		expiration vulnerability exists in the "Fish Hunt FL" iOS app version 3.8.0 and earlier, which allows a remote attacker to reuse, spoof, or steal other user and	N/A	A-MYF-FISH- 170921/245
Nextcloud					
circles	1				
Improper Neutralizati on of Input During Web Page Generation ('Cross-site Scripting')	ircles ircles mproper leutralizati n of Input During Web age Generation 'Cross-site cripting')		Nextcloud Circles is an open source social network built for the nextcloud ecosystem. In affected versions the Nextcloud Circles application is vulnerable to a stored Cross-Site Scripting (XSS) vulnerability. Due the strict Content-Security-Policy shipped with Nextcloud, this issue is not exploitable on modern browsers supporting Content-Security-Policy. It is recommended that the	https://githu b.com/nextcl oud/security- advisories/se curity/adviso ries/GHSA- hgpq-28gj- jrj9, https://githu b.com/nextcl oud/circles/c ommit/dbb9 7a83ccb342c 839a54f088a	A-NEX-CIRC- 170921/246

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
			Nextcloud Circles application is upgraded to 0.21.3, 0.20.10 or 0.19.14 to resolve this issue. As a workaround users may use a browser that has support for Content-Security- Policy. A notable exemption is Internet Explorer which does not support CSP properly. CVE ID : CVE-2021-32782	a19b8ba6844 b0e	
Authorizatio n Bypass Through User- Controlled Key	ypass rough er- htrolled		Nextcloud Circles is an open source social network built for the nextcloud ecosystem. In affected versions the Nextcloud Circles application allowed any user to join any "Secret Circle" without approval by the Circle owner leaking private information. It is recommended that Nextcloud Circles is upgraded to 0.19.15, 0.20.11 or 0.21.4. There are no workarounds for this issue.	https://githu b.com/nextcl oud/security- advisories/se curity/adviso ries/GHSA- 56j9-3rj4- wvgm, https://githu b.com/nextcl oud/circles/p ull/768	A-NEX-CIRC- 170921/247
deck					
Authorizatio n Bypass Through User- Controlled Key	07-Sep-21	ep-21 4 Deck is an open source kanban style organization tool aimed at personal planning and project organization for teams integrated with Nextcloud. affected versions the Deck application didn't properly check membership of users in a Circle. This allowed oth users in the instance to gain access to boards that have		https://githu b.com/nextcl oud/security- advisories/se curity/adviso ries/GHSA- 4mxp-j277- 82hr, https://githu b.com/nextcl oud/deck/pu	A-NEX-DECK- 170921/248

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			been shared with a Circle, even if the user was not a member of the circle. It is recommended that Nextcloud Deck is upgraded to 1.5.1, 1.4.4 or 1.2.9. If you are unable to update it is advised to disable the Deck plugin. CVE ID : CVE-2021-37631	ll/3217	
nextcloud					
Generation of Error Message Containing Sensitive Information	07-Sep-21	5	Nextcloud Text is an open source plaintext editing application which ships with the nextcloud server. In affected versions the Nextcloud Text application returned different error messages depending on whether a folder existed in a public link share. This is problematic in case the public link share has been created with "Upload Only" privileges. (aka "File Drop"). A link share recipient is not expected to see which folders or files exist in a "File Drop" share. Using this vulnerability an attacker is able to enumerate folders in such a share. Exploitation requires that the attacker has access to a valid affected "File Drop" link share. It is recommended that the Nextcloud Server is upgraded to 20.0.12, 21.0.4 or 22.0.1. Users who are unable to upgrade are advised to	https://githu b.com/nextcl oud/security- advisories/se curity/adviso ries/GHSA- gcf3-3wmc- 88jr, https://githu b.com/nextcl oud/text/pull /1716	A-NEX-NEXT- 170921/249

	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
			disable the Nextcloud Text application in the app settings. CVE ID : CVE-2021-32766		
Missing Authenticati on for Critical Function	07-Sep-21	6.4	Nextcloud server is an open source, self hosted personal cloud. In affected versions an attacker is able to bypass Two Factor Authentication in Nextcloud. Thus knowledge of a password, or access to a WebAuthN trusted device of a user was sufficient to gain access to an account. It is recommended that the Nextcloud Server is upgraded to 20.0.12, 21.0.4 or 22.1.0. There are no workaround for this vulnerability. CVE ID : CVE-2021-32800	https://githu b.com/nextcl oud/security- advisories/se curity/adviso ries/GHSA- gv5w-8q25- 785v, https://githu b.com/nextcl oud/server/p ull/28078	A-NEX-NEXT- 170921/250
Insertion of Sensitive Information into Log File	07-Sep-21	2.1	Nextcloud server is an open source, self hosted personal cloud. In affected versions logging of exceptions may have resulted in logging potentially sensitive key material for the Nextcloud Encryption-at-Rest functionality. It is recommended that the Nextcloud Server is upgraded to 20.0.12, 21.0.4 or 22.1.0. If upgrading is not an option users are advised to disable system logging to resolve this issue until such time that an upgrade can be performed Note that ff you do not use the Encryption-at-Rest	https://githu b.com/nextcl oud/security- advisories/se curity/adviso ries/GHSA- mcpf-v65v- 359h	A-NEX-NEXT- 170921/251
CVSS Scoring Sc	ale 0-1	1-2	2-3 3-4 4-5 5-6	6-7 7-8	8-9 9-10

Page 93 of 1474

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Inclusion of Functionalit y from Untrusted Control Sphere	07-Sep-21	10	<pre>functionality of Nextcloud you are not affected by this bug. CVE ID : CVE-2021-32801 Nextcloud server is an open source, self hosted personal cloud. Nextcloud supports rendering image previews for user provided file content. For some image types, the Nextcloud server was invoking a third-party library that wasn't suited for untrusted user-supplied content. There are several security concerns with passing user-generated content to this library, such as Server-Side-Request- Forgery, file disclosure or potentially executing code on the system. The risk depends on your system configuration and the installed library version. It is recommended that the Nextcloud Server is upgraded to 20.0.12, 21.0.4 or 22.1.0. These versions do not use this library anymore. As a workaround users may disable previews by setting `enable_previews` to `false` in `config.php`. CVE ID : CVE-2021-32802</pre>	https://githu b.com/nextcl oud/security- advisories/se curity/adviso ries/GHSA- m682-v4g9- wrq7, https://docs. nextcloud.co m/server/21 /admin_man ual/configura tion_files/pre views_config uration.html# disabling- previews	A-NEX-NEXT- 170921/252
richdocumen	its				
Authorizatio n Bypass Through User-	07-Sep-21	5	Nextcloud Richdocuments is an open source collaborative office suite. In affected versions the File Drop	https://githu b.com/nextcl oud/security- advisories/se	A-NEX-RICH- 170921/253
CVSS Scoring Sco	ale 0-1	1-2	2-3 3-4 4-5 5-6 Page 94 of 1474	6-7 7-8	8-9 <u>9-10</u>

Page 94 of 1474

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Controlled Key			features ("Upload Only" public link shares in Nextcloud) can be bypassed using the Nextcloud Richdocuments app. An attacker was able to read arbitrary files in such a share. It is recommended that the Nextcloud Richdocuments is upgraded to 3.8.4 or 4.2.1. If upgrading is not possible then it is recommended to disable the Richdocuments application. CVE ID : CVE-2021-37628	curity/adviso ries/GHSA- pxhh-954f- 8w7w, https://githu b.com/nextcl oud/richdocu ments/pull/1 664	
Allocation of Resources Without Limits or Throttling	07-Sep-21	5	Nextcloud Richdocuments is an open source collaborative office suite. In affected versions there is a lack of rate limiting on the Richdocuments OCS endpoint. This may have allowed an attacker to enumerate potentially valid share tokens. It is recommended that the Nextcloud Richdocuments app is upgraded to either 3.8.4 or 4.2.1 to resolve. For users unable to upgrade it is recommended that the Richdocuments application be disabled. CVE ID : CVE-2021-37629	https://githu b.com/nextcl oud/security- advisories/se curity/adviso ries/GHSA- gvvr-h36p- 8mjx	A-NEX-RICH- 170921/254
objection_pr	oject				
objection					
Improperly Controlled	06-Sep-21	7.5	objection.js is vulnerable to Improperly Controlled	https://huntr .dev/bounties	A-OBJ-OBJE- 170921/255
CVSS Scoring Sc	cale 0-1	1-2	2-3 3-4 4-5 5-6 Page 95 of 1474	6-7 7-8	8-9 9-10

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Modification of Dynamically -Determined Object Attributes			Modification of Object Prototype Attributes ('Prototype Pollution') CVE ID : CVE-2021-3766	/c98e0f0e- ebf2-4072- be73- a1848ea031c c, https://githu b.com/vincit/ objection.js/c ommit/b41aa b8dcd78f426 f7468dcda54 1a7aca18a66 a6	
onyaktech_co			ct		
onyaktech_co	omments_pro)		1	
Improper Neutralizati on of Input During Web Page Generation ('Cross-site Scripting')	07-Sep-21	3.5	An issue was discovered in CommentsService.ashx in OnyakTech Comments Pro 3.8. The comment posting functionality allows an attacker to add an XSS payload to the JSON request that will execute when users visit the page with the comment. CVE ID : CVE-2021-33483	N/A	A-ONY-ONYA- 170921/256
Use of Hard- coded Credentials	07-Sep-21	5	An issue was discovered in CommentsService.ashx in OnyakTech Comments Pro 3.8. An attacker can download a copy of the installer, decompile it, and discover a hardcoded IV used to encrypt the username and userid in the comment POST request. Additionally, the attacker can decrypt the encrypted encryption key (sent as a parameter in the	N/A	A-ONY-ONYA- 170921/257

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			comment form request) by setting this encrypted value as the username, which will appear on the comment page in its decrypted form. Using these two values (combined with the encryption functionality discovered in the decompiled installer), the attacker can encrypt another user's ID and username. These values can be used as part of the comment posting request in order to spoof the user. CVE ID : CVE-2021-33484		
Open-emr					
openemr					
Insertion of Sensitive Information into Log File	01-Sep-21	4	OpenEMR 6.0.0 has a pnotes_print.php?noteid= Insecure Direct Object Reference vulnerability via which an attacker can read the messages of all users. CVE ID : CVE-2021-40352	https://www. open- emr.org/wiki /index.php/S ecuring_Open EMR	A-OPE-OPEN- 170921/258
opensis_proj	ect			L	
opensis					
Improper Neutralizati on of Special Elements used in an SQL Command ('SQL Injection')	01-Sep-21	7.5	A SQL Injection vulnerability exists in openSIS 8.0 when MySQL (MariaDB) is being used as the application database. A malicious attacker can issue SQL commands to the MySQL (MariaDB) database through the NamesList.php str parameter.	N/A	A-OPE-OPEN- 170921/259

CVSS Scoring Scale	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10
Page 97 of 1474										

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2021-39378		
Opensuse					
libsolv					
Out-of- bounds Write	02-Sep-21	5	Buffer overflow vulnerability in function pool_installable in src/repo.h in libsolv before 0.7.17 allows attackers to cause a Denial of Service. CVE ID : CVE-2021-33928	N/A	A-OPE-LIBS- 170921/260
Out-of- bounds Write	02-Sep-21	5	Buffer overflow vulnerability in function pool_disabled_solvable in src/repo.h in libsolv before 0.7.17 allows attackers to cause a Denial of Service. CVE ID : CVE-2021-33929	N/A	A-OPE-LIBS- 170921/261
Out-of- bounds Write	02-Sep-21	5	Buffer overflow vulnerability in function pool_installable_whatprovide s in src/repo.h in libsolv before 0.7.17 allows attackers to cause a Denial of Service.	N/A	A-OPE-LIBS- 170921/262
Out-of- bounds Write	02-Sep-21	5	CVE ID : CVE-2021-33930 Buffer overflow vulnerability in function prune_to_recommended in src/policy.c in libsolv before 0.7.17 allows attackers to cause a Denial of Service. CVE ID : CVE-2021-33938	N/A	A-OPE-LIBS- 170921/263
os4ed					
opensis					
Improper Neutralizati on of Special	01-Sep-21	7.5	A SQL Injection vulnerability exists in openSIS 8.0 when MySQL (MariaDB) is being	N/A	A-OS4-OPEN- 170921/264
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 & CVE ID	Patch	NCIIPC ID
Elements used in an SQL Command ('SQL Injection')			used as the application database. A malicious attacker can issue SQL commands to the MySQL (MariaDB) database through the index.php username parameter. CVE ID : CVE-2021-39377		
Improper Neutralizati on of Special Elements used in an SQL Command ('SQL Injection')	01-Sep-21	7.5	A SQL Injection vulnerability exists in openSIS 8.0 when MySQL (MariaDB) is being used as the application database. A malicious attacker can issue SQL commands to the MySQL (MariaDB) database through the ResetUserInfo.php password_stn_id parameter. CVE ID : CVE-2021-39379	N/A	A-OS4-OPEN- 170921/265
Improper Neutralizati on of Special Elements used in an SQL Command ('SQL Injection')	01-Sep-21	7.5	A SQL injection vulnerability exists in version 8.0 of openSIS when MySQL or MariaDB is used as the application database. An attacker can then issue the SQL command through the index.php USERNAME parameter. NOTE: this issue may exist because of an incomplete fix for CVE-2020- 6637. CVE ID : CVE-2021-40353	N/A	A-OS4-OPEN- 170921/266
Otrs					
otrs					
N/A	06-Sep-21	5	It's possible to create an email which can be stuck while being processed by PostMaster filters, causing	https://otrs.c om/release- notes/otrs- security-	A-OTR-OTRS- 170921/267
CVSS Scoring Sc	ale 0-1	1-2	2-3 3-4 4-5 5-6 Page 99 of 1474	6-7 7-8	8-9 9-10

Page 99 of 1474

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			DoS. This issue affects: OTRS AG ((OTRS)) Community Edition 6.0.x version 6.0.1 and later versions. OTRS AG OTRS 7.0.x version 7.0.28 and prior versions; 8.0.x version 8.0.15 and prior versions. CVE ID : CVE-2021-36093	advisory- 2021-16/	
Improper Neutralizati on of Input During Web Page Generation ('Cross-site Scripting')	06-Sep-21	3.5	It's possible to craft a request for appointment edit screen, which could lead to the XSS attack. This issue affects: OTRS AG ((OTRS)) Community Edition 6.0.x version 6.0.1 and later versions. OTRS AG OTRS 7.0.x version 7.0.28 and prior versions. CVE ID : CVE-2021-36094	https://otrs.c om/release- notes/otrs- security- advisory- 2021-17/	A-OTR-OTRS- 170921/268
Weak Password Recovery Mechanism for Forgotten Password	06-Sep-21	5	Malicious attacker is able to find out valid user logins by using the "lost password" feature. This issue affects: OTRS AG ((OTRS)) Community Edition version 6.0.1 and later versions. OTRS AG OTRS 7.0.x version 7.0.28 and prior versions. CVE ID : CVE-2021-36095	https://otrs.c om/release- notes/otrs- security- advisory- 2021-18/	A-OTR-OTRS- 170921/269
Cleartext Storage of Sensitive Information	06-Sep-21	4	Generated Support Bundles contains private S/MIME and PGP keys if containing folder is not hidden. This issue affects: OTRS AG ((OTRS)) Community Edition 6.0.x version 6.0.1 and later versions. OTRS AG OTRS 7.0.x version 7.0.28 and prior	https://otrs.c om/release- notes/otrs- security- advisory- 2021-10/	A-OTR-OTRS- 170921/270

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
			versions; 8.0.x version 8.0.15 and prior versions.		
			CVE ID : CVE-2021-36096		
Owncloud					
owncloud					
Improper Privilege Managemen t	07-Sep-21	7.5	A receiver of a federated share with access to the database with ownCloud version before 10.8 could update the permissions and therefore elevate their own permissions. CVE ID : CVE-2021-35946	https://ownc loud.com/sec urity- advisories/cv e-2021- 35946/, https://doc.o wncloud.com /server/admi n_manual/rel ease_notes.ht ml	A-OWN- OWNC- 170921/271
Generation of Error Message Containing Sensitive Information	07-Sep-21	5	The public share controller in the ownCloud server before version 10.8.0 allows a remote attacker to see the internal path and the username of a public share by including invalid characters in the URL. CVE ID : CVE-2021-35947	https://ownc loud.com/sec urity- advisories/cv e-2021- 35947/, https://doc.o wncloud.com /server/admi n_manual/rel ease_notes.ht ml	A-OWN- OWNC- 170921/272
Incorrect Authorizatio n	07-Sep-21	5	The shareinfo controller in the ownCloud Server before 10.8.0 allows an attacker to bypass the permission checks for upload only shares and list metadata about the share. CVE ID : CVE-2021-35949	https://ownc loud.com/sec urity- advisories/cv e-2021- 35949/, https://doc.o wncloud.com /server/admi	A-OWN- OWNC- 170921/273

CVSS Scoring Scale

0-1

1-2

9-10

6-7

5-6

4-5

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID	
				n_manual/rel ease_notes.ht ml		
parity						
frontier						
Improper Input Validation	03-Sep-21	5	Frontier is Substrate's Ethereum compatibility layer. Prior to commit number Ob962f218f0cdd796dadfe26 c3f09e68f7861b26, a bug in `pallet-ethereum` can cause invalid transactions to be included in the Ethereum block state in `pallet- ethereum` due to not validating the input data size. Any invalid transactions included this way have no possibility to alter the internal Ethereum or Substrate state. The transaction will appear to have be included, but is of no effect as it is rejected by the EVM engine. The impact is further limited by Substrate extrinsic size constraints. A patch is available in commit number Ob962f218f0cdd796dadfe26 c3f09e68f7861b26. There are no workarounds aside from applying the patch. CVE ID : CVE-2021-39193	https://githu b.com/parityt ech/frontier/ pull/465/co mmits/8a2b8 90a2fb477d5 fedd0e4335b 0062383284 9ae, https://githu b.com/parityt ech/frontier/ pull/465, https://githu b.com/parityt ech/frontier/ security/advi sories/GHSA- hw4v-5x4h- c3xm	A-PAR-FRON- 170921/274	
parseplatform						
parse-server	parse-server					
Improper	02-Sep-21	5	Parse Server is an open	https://jira.m	A-PAR-PARS-	
CVSS Scoring Sca	le 0-1	1-2	2-3 3-4 4-5 5-6 Page 102 of 1474	6-7 7-8	8-9 9-10	

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Handling of Exceptional Conditions			source backend that can be deployed to any infrastructure that can run Node.js. Prior to version 4.10.3, Parse Server crashes when if a query request contains an invalid value for the `explain` option. This is due to a bug in the MongoDB Node.js driver which throws an exception that Parse Server cannot catch. There is a patch for this issue in version 4.10.3. No workarounds aside from upgrading are known to exist. CVE ID : CVE-2021-39187	ongodb.org/b rowse/NODE -3463, https://githu b.com/parse- community/p arse- server/comm it/308668c89 474223e244 8be92d6823 b52c1c313ec, https://githu b.com/parse- community/p arse- server/securi ty/advisories /GHSA-xqp8- w826-hh6x	170921/275
pcapture_pro	oject				
pcapture					
Improper Authenticati on	07-Sep-21	6.8	pcapture is an open source dumpcap web service interface . In affected versions this vulnerability allows an authenticated but unprivileged user to use the REST API to capture and download packets with no capture filter and without adequate permissions. This is important because the capture filters can effectively limit the scope of information that a user can see in the data captures. If no filter is present, then all data on the local network segment where	https://githu b.com/jdhwp gmbca/pcapt ure/security/ advisories/G HSA-3r67- fxpr-p2qx, https://githu b.com/jdhwp gmbca/pcapt ure/issues/7, https://githu b.com/jdhwp gmbca/pcapt ure/commit/ 0f74f431e09 70a2e5784db	A-PCA-PCAP- 170921/276

CVSS Scoring Scale	0-1	1-2	2-3	3-4	4-5
			_		-

6-7

5-6

7-8

8-9

9-10

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID		
			the program is running can be captured and downloaded. v3.12 fixes this problem. There is no workaround, you must upgrade to v3.12 or greater.	d955cfa4760 e3b1ef7			
			CVE ID : CVE-2021-39196				
phpmywind							
phpmywind							
Improper Control of Generation of Code ('Code Injection')	07-Sep-21	6.5	PHPMyWind 5.6 is vulnerable to Remote Code Execution. Becase input is filtered without "<, >, ?, =, `," In WriteConfig() function, an attacker can inject php code to /include/config.cache.php file. CVE ID : CVE-2021-39503	N/A	A-PHP-PHPM- 170921/277		
Pimcore							
pimcore							
Improper Neutralizati on of Input During Web Page Generation ('Cross-site Scripting')	01-Sep-21	3.5	Pimcore is an open source data & experience management platform. Prior to version 10.1.2, text-values were not properly escaped before printed in the version preview. This allowed XSS by authenticated users with access to the resources. This issue is patched in Pimcore version 10.1.2. CVE ID : CVE-2021-39166	https://githu b.com/pimco re/pimcore/s ecurity/advis ories/GHSA- w6j8-jc36- x5q9, https://githu b.com/pimco re/pimcore/p ull/10170	A-PIM-PIMC- 170921/278		
Improper Neutralizati on of Input During Web	01-Sep-21	3.5	Pimcore is an open source data & experience management platform. Prior to version 10.1.2, an	https://githu b.com/pimco re/pimcore/p ull/10178.pat	A-PIM-PIMC- 170921/279		
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		
Page Generation ('Cross-site Scripting')			authenticated user could add XSS code as a value of custom metadata on assets. There is a patch for this issue in Pimcore version 10.1.2. As a workaround, users may apply the patch manually. CVE ID : CVE-2021-39170	ch, https://githu b.com/pimco re/pimcore/p ull/10178, https://githu b.com/pimco re/pimcore/s ecurity/advis ories/GHSA- 2v88-qq7x- xq5f, https://huntr .dev/bounties /e4cb9cd8- 89cf-427c- 8d2e- 37ca40099bf 2/			
proto_projec	t						
proto							
N/A	01-Sep-21	5	This affects all versions of package Proto. It is possible to inject pollute the object property of an application using Proto by leveraging the merge function. CVE ID : CVE-2021-23426	N/A	A-PRO-PROT- 170921/280		
Puppet							
puppet							
Insertion of Sensitive Information into Log File	07-Sep-21	4	A flaw was discovered in bolt-server and ace where running a task with sensitive parameters results in those sensitive parameters being logged when they should not be. This issue only affects SSH/WinRM nodes	https://pupp et.com/securi ty/cve/CVE- 2021-27022/	A-PUP-PUPP- 170921/281		
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			
			(inventory service nodes).					
			CVE ID : CVE-2021-27022					
Pureftpd								
pure-ftpd								
Unrestricted Upload of File with Dangerous Type	05-Sep-21	5	In Pure-FTPd 1.0.49, an incorrect max_filesize quota mechanism in the server allows attackers to upload files of unbounded size, which may lead to denial of service or a server hang. This occurs because a certain greater-than-zero test does not anticipate an initial -1 value.	N/A	A-PUR-PURE- 170921/282			
			CVE ID : CVE-2021-40524					
Python	1							
pillow								
Out-of- bounds Read	03-Sep-21	5	The package pillow from 0 and before 8.3.2 are vulnerable to Regular Expression Denial of Service (ReDoS) via the getrgb function. CVE ID : CVE-2021-23437	https://pillo w.readthedoc s.io/en/stabl e/releasenote s/8.3.2.html, https://githu b.com/pytho n- pillow/Pillow /commit/9e0 8eb8f78fdfd2 f476e1b20b7 cf386837548 66b, https://snyk.i o/vuln/SNYK -PYTHON- PILLOW- 1319443	A-PYT-PILL- 170921/283			

CVSS Scoring Scale	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10
			P	age 106 c	of 1474					

Weakness	Publish Date	sh Date CVSS Description & CVE ID		Patch	NCIIPC ID				
redux									
gutenberg_template_library_\\&_redux_framework									
Incorrect Authorizatio n	02-Sep-21	2-Sep-21 4 The Gutenberg Template Library & Redux Framework plugin <= 4.2.11 for WordPress used an incorrect authorization check in the REST API endpoints registered under the "redux/v1/templates/" REST Route in "redux- templates/classes/class- api.php". The `permissions_callback` used in this file only checked for the `edit_posts` capability which is granted to lower- privileged users such as contributors, allowing such users to install arbitrary plugins from the WordPress repository and edit arbitrary posts. CVE ID : CVE-2021-38312		N/A	A-RED-GUTE- 170921/284				
N/A	02-Sep-21	5	The Gutenberg Template Library & Redux Framework plugin <= 4.2.11 for WordPress registered several AJAX actions available to unauthenticated users in the `includes` function in `redux- core/class-redux-core.php` that were unique to a given site but deterministic and predictable given that they were based on an md5 hash of the site URL with a known salt value of '-redux' and an md5 hash of the previous	N/A	A-RED-GUTE- 170921/285				
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 & CVE ID	Patch	NCIIPC ID								
			hash with a known salt value of '-support'. These AJAX actions could be used to retrieve a list of active plugins and their versions, the site's PHP version, and an unsalted md5 hash of site's `AUTH_KEY` concatenated with the `SECURE_AUTH_KEY`. CVE ID : CVE-2021-38314										
remark					<u> </u>								
remark-htm	l												
Improper Neutralizati on of Input During Web Page Generation ('Cross-site Scripting')	07-Sep-21	4.3	remark-html is an open source nodejs library which compiles Markdown to HTML. In affected versions the documentation of remark-html has mentioned that it was safe by default. In practice the default was never safe and had to be opted into. That is, user input was not sanitized. This means arbitrary HTML can be passed through leading to potential XSS attacks. The problem has been patched in 13.0.2 and 14.0.1: `remark- html` is now safe by default, and the implementation matches the documentation. On older affected versions, pass `sanitize: true` if you cannot update. CVE ID : CVE-2021-39199	https://githu b.com/remar kjs/remark- html/releases /tag/14.0.1, https://githu b.com/remar kjs/remark- html/security /advisories/G HSA-9q5w- 79cv-947m, https://githu b.com/remar kjs/remark- html/commit /b75c9dde58 2ad87ba498e 369c033dc8a 350478c1	A-REM- REMA- 170921/286								
Samsung													
drive_manager													
CVSS Scoring Sc	ale 0-1	1-2	2-3 3-4 4-5 5-6 Page 108 of 1474	6-7 7-8	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
Incorrect Authorizatio n	01-Sep-21	4.6	Samsung Drive Manager 2.0.104 on Samsung H3 devices allows attackers to bypass intended access controls on disk management. WideCharToMultiByte, WideCharStr, and MultiByteStr can contribute to password exposure. CVE ID : CVE-2021-39373	N/A	A-SAM-DRIV- 170921/287
Schneider-el	ectric				
gp-pro_ex					
Uncontrolle d Search Path Element	02-Sep-21	4.4	A CWE-427: Uncontrolled Search Path Element vulnerability exists in GP-Pro EX,V4.09.250 and prior, that could cause local code execution with elevated privileges when installing the software. CVE ID : CVE-2021-22775	https://down load.schneide r- electric.com/f iles?p_Doc_Re f=SEVD- 2021-222-03	A-SCH-GP-P- 170921/288
simple wate	r refilling sta	tion n	nanagement_system_project		
			nanagement_system		
Improper Neutralizati on of Special Elements used in an SQL Command ('SQL Injection')	07-Sep-21	7.5	SQL Injection can occur in Simple Water Refilling Station Management System 1.0 via the water_refilling/classes/Login .php username parameter. CVE ID : CVE-2021-38840	N/A	A-SIM-SIMP- 170921/289
Unrestricted Upload of File with Dangerous	07-Sep-21	6.5	Remote Code Execution can occur in Simple Water Refilling Station Management System 1.0 via the System	N/A	A-SIM-SIMP- 170921/290

CVSS Scoring Scale	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10
			D	- 	f 1/7/					

Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
		Logo option on the system_info page in classes/SystemSettings.php with an update_settings action.		
		CVE ID : CVE-2021-38841		
				Γ
06-Sep-21	7.5	Sketch before 75 mishandles external library feeds. CVE ID : CVE-2021-40531	https://www. sketch.com/u pdates/#vers ion-75	A-SKE-SKET- 170921/291
6			<u> </u>	I
08-Sep-21	3.5	SmarterTools SmarterMail 16.x before build 7866 has stored XSS. The application fails to sanitize email content, thus allowing one to inject HTML and/or JavaScript into a page that will then be processed and stored by the application. CVE ID : CVE-2021-40377	https://www. smartertools. com/smarter mail/release- notes/curren t	A-SMA-SMAR- 170921/292
I			L	
m				
01-Sep-21	6.5	Insecure deserialization leading to Remote Code Execution was detected in the Orion Platform version 2020.2.5. Authentication is required to exploit this vulnerability. CVE ID : CVE-2021-35215	https://docu mentation.sol arwinds.com/ en/success_c enter/orionpl atform/conte nt/core- secure- configuration. htm, https://www.	A-SOL-ORIO- 170921/293
	06-Sep-21 08-Sep-21	Image: select of the select	Image: constraint of the system_info page in classes/SystemSettings.php with an update_settings action.CVE ID : CVE-2021-3884106-Sep-217.5Sketch before 75 mishandles external library feeds. CVE ID : CVE-2021-4053106-Sep-217.5SmarterTools SmarterMail 16.x before build 7866 has stored XSS. The application fails to sanitize email content, thus allowing one to inject HTML and/or JavaScript into a page that will then be processed and stored by the application. CVE ID : CVE-2021-4037708-Sep-213.508-Sep-215.508-Sep-215.510-Sep-216.508-Sep-215.508-Sep-215.508-Sep-215.508-Sep-215.508-Sep-215.508-Sep-215.508-Sep-215.509-Sep-215.50	Image: Constraint of the system info page in classes/SystemSettings php with an update_settings action. CVE ID : CVE-2021-38841Image: Constraint of the system info page in classes/SystemSettings php with an update_settings action. CVE ID : CVE-2021-38841Image: Constraint of the system info page in classes/SystemSettings php with an update_settings action. CVE ID : CVE-2021-38841Image: Constraint of the system info page in classes/SystemSettings php with an update_settings action. CVE ID : CVE-2021-38841Image: Constraint of the system info page in classes/SystemSettings php with an update_settings action. Stetch.com/u pdates/#vers ion-7506-Sep-217.5Sketch before 75 mishandles external library feeds. CVE ID : CVE-2021-40531https://www. sketch.com/u pdates/#vers ion-7508-Sep-213.5SmarterTools SmarterMail 16.x before build 7866 has stored XSS. The application fails to sanitize email content, thus allowing one to inject HTML and/or JavaScript into a page that will then be processed and stored by the application. CVE ID : CVE-2021-40377https://www. smartertools. com/smarter mail/release-notes/curren t t01-Sep-216.5Insecure deserialization leading to Remote Code Execution was detected in the 0rion Platform version 2020.2.5. Authentication is required to exploit this vulnerability. CVE ID : CVE-2021-35215https://docu mentation. https://www. https://www.

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
				solarwinds.co m/trust- center/securi ty- advisories/cv e-2021- 35215	
Deserializati on of Untrusted Data	01-Sep-21	6.5	Deserialization of Untrusted Data in the Web Console Chart Endpoint can lead to remote code execution. An unauthorized attacker who has network access to the Orion Patch Manager Web Console could potentially exploit this and compromise the server CVE ID : CVE-2021-35218	https://docu mentation.sol arwinds.com/ en/success_c enter/patchm an/content/r elease_notes/ patchman_20 20-2- 6_release_not es.htm, https://www. solarwinds.co m/trust- center/securi ty- advisories/cv e-2021- 35218	A-SOL-ORIO- 170921/294
Improper Neutralizati on of Input During Web Page Generation ('Cross-site Scripting')	01-Sep-21	3.5	User with Orion Platform Admin Rights could store XSS through URL POST parameter in CreateExternalWebsite website. CVE ID : CVE-2021-35238	https://supp ort.solarwind s.com/Succes sCenter/s/art icle/Orion- Platform- 2020-2-6- Hotfix- 1?language=e n_US, https://docu mentation.sol arwinds.com/ en/success_c	A-SOL-ORIO- 170921/295
CVSS Scoring Sc	ale 0-1	1-2	2-3 3-4 4-5 5-6	6-7 7-8	8-9 9-10

Page 111 of 1474

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID			
sqlite-web_p	roject	<u>.</u>		I	L			
sqlite-web								
Cross-Site Request Forgery (CSRF)	08-Sep-21	6.8	This affects all versions of package sqlite-web. The SQL dashboard area allows sensitive actions to be performed without validating that the request originated from the application. This could enable an attacker to trick a user into performing these actions unknowingly through a Cross Site Request Forgery (CSRF) attack. CVE ID : CVE-2021-23404	N/A	A-SQL-SQLI- 170921/298			
swiftcrm	swiftcrm							
club-manage	ement-softwa	re						
Improper Neutralizati on of Special Elements used in an SQL Command ('SQL Injection')	06-Sep-21	6.5	An id GET parameter of the WordPress Membership SwiftCloud.io WordPress plugin through 1.0 is not properly sanitised, escaped or validated before inserting to a SQL statement, leading to SQL injection. CVE ID : CVE-2021-24392	N/A	A-SWI-CLUB- 170921/299			
Telegram								
web_k_alpha								
N/A	06-Sep-21	7.5	Telegram Web K Alpha before 0.7.2 mishandles the characters in a document extension. CVE ID : CVE-2021-40532	https://githu b.com/moret hanwords/tw eb/commit/f 224e459c36e b96b2cf9dba 559a48b1f08 d23330	A-TEL-WEB 170921/300			

CVSS Scoring Scale	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10
			P	age 113 c	of 1474					

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
terarecon		I		I	
aquariusnet					
Improper Privilege Managemen t	01-Sep-21	8.5	NMSAccess32.exe in TeraRecon AQNetClient 4.4.13 allows attackers to execute a malicious binary with SYSTEM privileges via a low-privileged user account. To exploit this, a low- privileged user must change the service configuration or overwrite the binary service. CVE ID : CVE-2021-35508	N/A	A-TER-AQUA- 170921/301
th-wildau				1	
covid-19_con	tact_tracing				
Improper Authenticati on	07-Sep-21	4	api/account/register in the TH Wildau COVID-19 Contact Tracing application through 2021-09-01 has Incorrect Access Control. An attacker can interfere with tracing of infection chains by creating 500 random users within 2500 seconds. CVE ID : CVE-2021-33831	https://www. th- wildau.de/stu dieren- weiterbilden/ neuigkeiten- und- veranstaltung en/corona/	A-THCOVI- 170921/302
Trendmicro	I			I	I
maximum_se	curity_2019				
Improper Privilege Managemen t	06-Sep-21	4.6	Trend Micro Security (Consumer) 2021 and 2020 are vulnerable to a directory junction vulnerability which could allow an attacker to exploit the system to escalate privileges and create a denial of service. CVE ID : CVE-2021-36744	https://helpc enter.trendmi cro.com/en- us/article/tm ka-10568	A-TRE-MAXI- 170921/303
			UVE ID : UVE-2021-30/44		

CVSS Scoring Scale	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10
			Pa	age 114 c	of 1474					

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID		
maximum_se	curity_2020						
Improper Privilege Managemen t	06-Sep-21	4.6	Trend Micro Security (Consumer) 2021 and 2020 are vulnerable to a directory junction vulnerability which could allow an attacker to exploit the system to escalate privileges and create a denial of service. CVE ID : CVE-2021-36744	https://helpc enter.trendmi cro.com/en- us/article/tm ka-10568	A-TRE-MAXI- 170921/304		
maximum_se	curity_2021				1		
Improper Privilege Managemen t	06-Sep-21	4.6	Trend Micro Security (Consumer) 2021 and 2020 are vulnerable to a directory junction vulnerability which could allow an attacker to exploit the system to escalate privileges and create a denial of service. CVE ID : CVE-2021-36744	https://helpc enter.trendmi cro.com/en- us/article/tm ka-10568	A-TRE-MAXI- 170921/305		
security_for_	best_buy						
Improper Privilege Managemen t	06-Sep-21	4.6	Trend Micro Security (Consumer) 2021 and 2020 are vulnerable to a directory junction vulnerability which could allow an attacker to exploit the system to escalate privileges and create a denial of service. CVE ID : CVE-2021-36744	https://helpc enter.trendmi cro.com/en- us/article/tm ka-10568	A-TRE-SECU- 170921/306		
trumani							
stop_spamm	stop_spammers						
Improper Neutralizati on of Input During Web Page	06-Sep-21	3.5	The Stop Spammers Security Block Spam Users, Comments, Forms WordPress plugin before 2021.18 does not escape	N/A	A-TRU-STOP- 170921/307		
CVSS Scoring Sc	ale 0-1	1-2	2-3 3-4 4-5 5-6 Page 115 of 1474	6-7 7-8	8-9 9-10		

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Generation ('Cross-site Scripting')			some of its settings, allowing high privilege users such as admin to set Cross-Site Scripting payloads in them even when the unfiltered_html capability is disallowed CVE ID : CVE-2021-24517		
typelevel					1
http4s					
Origin Validation Error	01-Sep-21	6.4	Http4s is a minimal, idiomatic Scala interface for HTTP services. In http4s versions 0.21.26 and prior, 0.22.0 through 0.22.2, 0.23.0, 0.23.1, and 1.0.0-M1 through 1.0.0-M24, the default CORS configuration is vulnerable to an origin reflection attack. The middleware is also susceptible to a Null Origin Attack. The problem is fixed in 0.21.27, 0.22.3, 0.23.2, and 1.0.0-M25. The original `CORS` implementation and `CORSConfig` are deprecated. See the GitHub GHSA for more information, including code examples and workarounds. CVE ID : CVE-2021-39185	https://githu b.com/http4s /http4s/secu rity/advisorie s/GHSA-52cf- 226f-rhr6	A-TYP-HTTP- 170921/308
ulfius_projec	t				
ulfius					
N/A	07-Sep-21	7.5	ulfius_uri_logger in Ulfius HTTP Framework before 2.7.4 omits con_info initialization and a con_info- >request NULL check for	https://githu b.com/babelo uest/ulfius/c ommit/c83f5 64c184a2714	A-ULF-ULFI- 170921/309
CVSS Scoring Sc	ale 0-1	1-2	2-3 3-4 4-5 5-6 Page 116 of 1474	6-7 7-8	8-9 9-10

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID	
			certain malformed HTTP requests. CVE ID : CVE-2021-40540	5e07c274b30 5cabe943bbf aa, https://githu b.com/babelo uest/ulfius/c ompare/v2.7. 3v2.7.4		
underconstru		t				
underconstru	iction			1	1	
Improper Neutralizati on of Input During Web Page Generation ('Cross-site Scripting')01-Sep-21The underConstruction plugin <= 1.18 for WordPress echoes out the raw value of `\$GLOBALS['PHP_SELF']` in the ucOptions.php file. On certain configurations including Apache+modPHP, this makes it possible to use it to perform a reflected Cross-Site Scripting attack by injecting malicious code in the request path.A-UND-UNDE- 170921/310						
versa-networ	⁻ ks					
versa_directo	or					
Improper Neutralizati on of Input During Web Page Generation ('Cross-site Scripting')	07-Sep-21	4.3	A XSS vulnerability exists in Versa Director Release: 16.1R2 Build: S8. An attacker can use the administration web interface URL to create a XSS based attack. CVE ID : CVE-2021-39285	https://versa - networks.co m	A-VER-VERS- 170921/311	
VIM						
vim						
Out-of- bounds	06-Sep-21	4.6	vim is vulnerable to Heap- based Buffer Overflow	https://githu b.com/vim/vi	A-VIM-VIM- 170921/312	
CVSS Scoring Sca	ale 0-1	1-2	2-3 3-4 4-5 5-6 Page 117 of 1474	6-7 7-8	8-9 9-10	

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Write			CVE ID : CVE-2021-3770	m/commit/b 7081e135a16 091c93f6f5f7 525a5c58fb7 ca9f9, https://huntr .dev/bounties /016ad2f2- 07c1-4d14- a8ce- 6eed1072936 5	
web-settler					
form_builder	•				
Improper Neutralizati on of Input During Web Page Generation ('Cross-site Scripting')	06-Sep-21	3.5	The Form Builder Create Responsive Contact Forms WordPress plugin before 1.9.8.4 does not sanitise or escape its Form Title, allowing high privilege users such as admin to set Cross- Site Scripting payload in them, even when the unfiltered_html capability is disallowed CVE ID : CVE-2021-24513	N/A	A-WEB- FORM- 170921/313
Weechat	<u> </u>				
weechat					
Out-of- bounds Read	05-Sep-21	5	WeeChat before 3.2.1 allows remote attackers to cause a denial of service (crash) via a crafted WebSocket frame that trigger an out-of-bounds read in plugins/relay/relay- websocket.c in the Relay plugin. CVE ID : CVE-2021-40516	https://weec hat.org/doc/s ecurity/, https://githu b.com/weech at/weechat/c ommit/8b13 31f98de1714 bae15a9ca2e 2b393ba49d	A-WEE- WEEC- 170921/314
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 & CVE ID	Patch	NCIIPC ID	
				735b		
wp-webhook	S			I	1	
email_encode	er					
Improper Neutralizati on of Input During Web Page Generation ('Cross-site Scripting')06-Sep-214.3		ep-21 4.3 The Email Encoder – Protect Email Addresses WordPress plugin before 2.1.2 has an endpoint that requires no authentication and will render a user supplied value in the HTML response without escaping or sanitizing the data. CVE ID : CVE-2021-24599		N/A	A-WPEMAI- 170921/315	
wpfront						
wpfront_noti	fication_bar					
Improper Neutralizati on of Input During Web Page Generation ('Cross-site Scripting')	eutralizati n of Input uring Web age06-Sep-213.5properly sanitise and escape its settings, which could allow high privilege users to perform Cross-Site Scripting attacks even when the unfiltered html capability is		N/A	A-WPF- WPFR- 170921/316		
zmartzone						
mod_auth_op	enidc					
URL Redirection to Untrusted Site ('Open Redirect')	03-Sep-21	5.8	mod_auth_openidc is an authentication/authorization module for the Apache 2.x HTTP server that functions as an OpenID Connect Relying Party, authenticating users against an OpenID Connect Provider. In versions prior to 2.4.9.4, the 3rd-party init SSO	https://githu b.com/zmart zone/mod_au th_openidc/c ommit/03e6b fb446f4e3f27 c003d30d6a4 33e5dd8e2b3 d,	A-ZMA-MOD 170921/317	
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 & CVE ID	Patch	NCIIPC ID
			functionality of mod_auth_openidc was reported to be vulnerable to an open redirect attack by supplying a crafted URL in the `target_link_uri` parameter. A patch in version 2.4.9.4 made it so that the `OIDCRedirectURLsAllowed` setting must be applied to the `target_link_uri` parameter. There are no known workarounds aside from upgrading to a patched version. CVE ID : CVE-2021-39191	https://githu b.com/zmart zone/mod_au th_openidc/s ecurity/advis ories/GHSA- 2pgf-8h6h- gqg2	
Zohocorp					
manageengii	ne_adselfserv	ice_plu	IS		
Improper Authenticati on	07-Sep-21	7.5	Zoho ManageEngine ADSelfService Plus version 6113 and prior is vulnerable to REST API authentication bypass with resultant remote code execution. CVE ID : CVE-2021-40539	https://www. manageengin e.com/produ cts/self- service- password/kb /how-to-fix- authenticatio n-bypass- vulnerability- in-REST- API.html, https://www. manageengin e.com	A-ZOH- MANA- 170921/318
manageengii	ne_servicedes	sk_plus			
Improper Authenticati on	01-Sep-21	7.5	Zoho ManageEngine ServiceDesk Plus before 11302 is vulnerable to authentication bypass that	https://www. manageengin e.com, https://www.	A-ZOH- MANA- 170921/319
CVSS Scoring Sc	ale 0-1	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	
Page 120 of 1474											

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			allows a few REST-API URLs without authentication. CVE ID : CVE-2021-37415	manageengin e.com/produ cts/service-	
				desk/on- premises/rea dme.html#11 302	
			Hardware		
actions-semi	l				
ats2815					
N/A	07-Sep-21	6.1	The Bluetooth Classic implementation on Actions ATS2815 and ATS2819 chipsets does not properly handle the reception of multiple LMP_host_connection_req packets, allowing attackers in radio range to trigger a denial of service (deadlock) of the device via crafted LMP packets. Manual user intervention is required to restart the device and restore Bluetooth communication. CVE ID : CVE-2021-31785	https://www. actions- semi.com/ind ex.php?id=35 81&siteId=4	H-ACT-ATS2- 170921/320
N/A	07-Sep-21	6.1	The Bluetooth Classic Audio implementation on Actions ATS2815 and ATS2819 devices does not properly handle a connection attempt from a host with the same BDAddress as the current connected BT host, allowing attackers to trigger a disconnection and deadlock of the device by connecting with a forged BDAddress that	https://www. actions- semi.com/ind ex.php?id=35 81&siteId=4	H-ACT-ATS2- 170921/321

CVSS Scoring Scale	0-1	1-2	2-

5-6

6-7

7-8

8-9

9-10

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			matches the original connected host.		
			CVE ID : CVE-2021-31786		
ats2819				L	L
N/A	07-Sep-21	6.1	The Bluetooth Classic implementation on Actions ATS2815 and ATS2819 chipsets does not properly handle the reception of multiple LMP_host_connection_req packets, allowing attackers in radio range to trigger a denial of service (deadlock) of the device via crafted LMP packets. Manual user intervention is required to restart the device and restore Bluetooth communication. CVE ID : CVE-2021-31785	https://www. actions- semi.com/ind ex.php?id=35 81&siteId=4	H-ACT-ATS2- 170921/322
N/A	07-Sep-21	6.1	The Bluetooth Classic Audio implementation on Actions ATS2815 and ATS2819 devices does not properly handle a connection attempt from a host with the same BDAddress as the current connected BT host, allowing attackers to trigger a disconnection and deadlock of the device by connecting with a forged BDAddress that matches the original connected host. CVE ID : CVE-2021-31786	https://www. actions- semi.com/ind ex.php?id=35 81&siteId=4	H-ACT-ATS2- 170921/323
ats2819p					
N/A	07-Sep-21	6.1	The Bluetooth Classic implementation on Actions	https://www. actions-	H-ACT-ATS2-
CVSS Scoring S	cale 0-1	1-2	2-3 3-4 4-5 5-6 Page 122 of 1474	6-7 7-8	8-9 9-10

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			ATS2815 and ATS2819 chipsets does not properly handle the reception of multiple LMP_host_connection_req packets, allowing attackers in radio range to trigger a denial of service (deadlock) of the device via crafted LMP packets. Manual user intervention is required to restart the device and restore Bluetooth communication. CVE ID : CVE-2021-31785	semi.com/ind ex.php?id=35 81&siteId=4	170921/324
N/A	07-Sep-21	6.1	The Bluetooth Classic Audio implementation on Actions ATS2815 and ATS2819 devices does not properly handle a connection attempt from a host with the same BDAddress as the current connected BT host, allowing attackers to trigger a disconnection and deadlock of the device by connecting with a forged BDAddress that matches the original connected host. CVE ID : CVE-2021-31786	https://www. actions- semi.com/ind ex.php?id=35 81&siteId=4	H-ACT-ATS2- 170921/325
ats2819s					
N/A	07-Sep-21	6.1	The Bluetooth Classic implementation on Actions ATS2815 and ATS2819 chipsets does not properly handle the reception of multiple LMP_host_connection_req packets, allowing attackers in radio range to trigger a	https://www. actions- semi.com/ind ex.php?id=35 81&siteId=4	H-ACT-ATS2- 170921/326
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 & CVE ID	Patch	NCIIPC ID
			denial of service (deadlock) of the device via crafted LMP packets. Manual user intervention is required to restart the device and restore Bluetooth communication. CVE ID : CVE-2021-31785		
N/A	07-Sep-21	6.1	The Bluetooth Classic Audio implementation on Actions ATS2815 and ATS2819 devices does not properly handle a connection attempt from a host with the same BDAddress as the current connected BT host, allowing attackers to trigger a disconnection and deadlock of the device by connecting with a forged BDAddress that matches the original connected host. CVE ID : CVE-2021-31786	https://www. actions- semi.com/ind ex.php?id=35 81&siteId=4	H-ACT-ATS2- 170921/327
ats2819t					
N/A	07-Sep-21	6.1	The Bluetooth Classic implementation on Actions ATS2815 and ATS2819 chipsets does not properly handle the reception of multiple LMP_host_connection_req packets, allowing attackers in radio range to trigger a denial of service (deadlock) of the device via crafted LMP packets. Manual user intervention is required to restart the device and restore Bluetooth communication.	https://www. actions- semi.com/ind ex.php?id=35 81&siteId=4	H-ACT-ATS2- 170921/328

CVSS Scoring Scale	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10	
Page 124 of 1/74											

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2021-31785		
N/A	07-Sep-21	6.1	The Bluetooth Classic Audioimplementation on ActionsATS2815 and ATS2819devices does not properlyhandle a connection attemptfrom a host with the sameBDAddress as the currentconnected BT host, allowingattackers to trigger adisconnection and deadlockof the device by connectingwith a forged BDAddress thatmatches the originalconnected host.		H-ACT-ATS2- 170921/329
			CVE ID : CVE-2021-31786		
Amazon					
kindle					
Integer Overflow or Wraparoun d	01-Sep-21	9.3	Amazon Kindle e-reader prior to and including version 5.13.4 contains an Integer Overflow that leads to a Heap-Based Buffer Overflow in function CJBig2Image::expand() and results in a memory corruption that leads to code execution when parsing a crafted PDF book. CVE ID : CVE-2021-30354	N/A	H-AMA-KIND- 170921/330
Improper Privilege Managemen t	01-Sep-21	9.3	Amazon Kindle e-reader prior to and including version 5.13.4 improperly manages privileges, allowing the framework user to elevate privileges to root. CVE ID : CVE-2021-30355	N/A	H-AMA-KIND- 170921/331

CV33 Scotting Scale		12	23	425		50	07	,0
CVSS Scoring Scale	0-1	1_2	2-3	3-1	1-5	5-6	6-7	7-8

8-9

9-10

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID			
Arubanetwo	Arubanetworks							
7005								
Improper Limitation of a Pathname to a Restricted Directory ('Path Traversal')	07-Sep-21	7.2	A local path traversal vulnerability was discovered in Aruba SD-WAN Software and Gateways; Aruba Operating System Software version(s): Prior to 8.6.0.0- 2.2.0.4; Prior to 8.7.1.1, 8.6.0.7, 8.5.0.12, 8.3.0.16. Aruba has released patches for Aruba SD-WAN Software and Gateways and ArubaOS that address this security vulnerability.	https://www. arubanetwor ks.com/asset s/alert/ARUB A-PSA-2021- 016.txt	H-ARU-7005- 170921/332			
			CVE ID : CVE-2021-37731					
7008								
Improper Limitation of a Pathname to a Restricted Directory ('Path Traversal')	07-Sep-21	7.2	A local path traversal vulnerability was discovered in Aruba SD-WAN Software and Gateways; Aruba Operating System Software version(s): Prior to 8.6.0.0- 2.2.0.4; Prior to 8.7.1.1, 8.6.0.7, 8.5.0.12, 8.3.0.16. Aruba has released patches for Aruba SD-WAN Software and Gateways and ArubaOS that address this security vulnerability. CVE ID : CVE-2021-37731	https://www. arubanetwor ks.com/asset s/alert/ARUB A-PSA-2021- 016.txt	H-ARU-7008- 170921/333			
7010				I	I			
Improper Limitation of a Pathname to a Restricted Directory	07-Sep-21	7.2	A local path traversal vulnerability was discovered in Aruba SD-WAN Software and Gateways; Aruba Operating System Software version(s): Prior to 8.6.0.0-	https://www. arubanetwor ks.com/asset s/alert/ARUB A-PSA-2021-	H-ARU-7010- 170921/334			
CVSS Scoring Sc	ale 0-1	1-2	2-3 3-4 4-5 5-6 Page 126 of 1474	6-7 7-8	8-9 9-10			

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
('Path Traversal')			2.2.0.4; Prior to 8.7.1.1, 8.6.0.7, 8.5.0.12, 8.3.0.16. Aruba has released patches for Aruba SD-WAN Software and Gateways and ArubaOS that address this security vulnerability. CVE ID : CVE-2021-37731	016.txt	
7024	I			l	
Improper Limitation of a Pathname to a Restricted Directory ('Path Traversal')	07-Sep-21	7.2	A local path traversal vulnerability was discovered in Aruba SD-WAN Software and Gateways; Aruba Operating System Software version(s): Prior to 8.6.0.0- 2.2.0.4; Prior to 8.7.1.1, 8.6.0.7, 8.5.0.12, 8.3.0.16. Aruba has released patches for Aruba SD-WAN Software and Gateways and ArubaOS that address this security vulnerability. CVE ID : CVE-2021-37731	https://www. arubanetwor ks.com/asset s/alert/ARUB A-PSA-2021- 016.txt	H-ARU-7024- 170921/335
7030			L		
Improper Limitation of a Pathname to a Restricted Directory ('Path Traversal')	07-Sep-21	7.2	A local path traversal vulnerability was discovered in Aruba SD-WAN Software and Gateways; Aruba Operating System Software version(s): Prior to 8.6.0.0- 2.2.0.4; Prior to 8.7.1.1, 8.6.0.7, 8.5.0.12, 8.3.0.16. Aruba has released patches for Aruba SD-WAN Software and Gateways and ArubaOS that address this security vulnerability. CVE ID : CVE-2021-37731	https://www. arubanetwor ks.com/asset s/alert/ARUB A-PSA-2021- 016.txt	H-ARU-7030- 170921/336
CVSS Scoring Sc	ale 0-1	1-2	2-3 3-4 4-5 5-6 Page 127 of 1474	6-7 7-8	8-9 9-10

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID			
7205	7205							
Improper Limitation of a Pathname to a Restricted Directory ('Path Traversal')	07-Sep-21	7.2	A local path traversal vulnerability was discovered in Aruba SD-WAN Software and Gateways; Aruba Operating System Software version(s): Prior to 8.6.0.0- 2.2.0.4; Prior to 8.7.1.1, 8.6.0.7, 8.5.0.12, 8.3.0.16. Aruba has released patches for Aruba SD-WAN Software and Gateways and ArubaOS that address this security vulnerability. CVE ID : CVE-2021-37731	https://www. arubanetwor ks.com/asset s/alert/ARUB A-PSA-2021- 016.txt	H-ARU-7205- 170921/337			
7210				<u> </u>				
Improper Limitation of a Pathname to a Restricted Directory ('Path Traversal')	07-Sep-21	7.2	A local path traversal vulnerability was discovered in Aruba SD-WAN Software and Gateways; Aruba Operating System Software version(s): Prior to 8.6.0.0- 2.2.0.4; Prior to 8.7.1.1, 8.6.0.7, 8.5.0.12, 8.3.0.16. Aruba has released patches for Aruba SD-WAN Software and Gateways and ArubaOS that address this security vulnerability. CVE ID : CVE-2021-37731	https://www. arubanetwor ks.com/asset s/alert/ARUB A-PSA-2021- 016.txt	H-ARU-7210- 170921/338			
7220								
Improper Limitation of a Pathname to a Restricted Directory ('Path	07-Sep-21	7.2	A local path traversal vulnerability was discovered in Aruba SD-WAN Software and Gateways; Aruba Operating System Software version(s): Prior to 8.6.0.0- 2.2.0.4; Prior to 8.7.1.1,	https://www. arubanetwor ks.com/asset s/alert/ARUB A-PSA-2021- 016.txt	H-ARU-7220- 170921/339			
CVSS Scoring Sc	ale 0-1	1-2	2-3 3-4 4-5 5-6 Page 128 of 1474	6-7 7-8	8-9 9-10			

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Traversal')			8.6.0.7, 8.5.0.12, 8.3.0.16. Aruba has released patches for Aruba SD-WAN Software and Gateways and ArubaOS that address this security vulnerability. CVE ID : CVE-2021-37731		
7240xm	I			I	
Improper Limitation of a Pathname to a Restricted Directory ('Path Traversal')	07-Sep-21	7.2	A local path traversal vulnerability was discovered in Aruba SD-WAN Software and Gateways; Aruba Operating System Software version(s): Prior to 8.6.0.0- 2.2.0.4; Prior to 8.7.1.1, 8.6.0.7, 8.5.0.12, 8.3.0.16. Aruba has released patches for Aruba SD-WAN Software and Gateways and ArubaOS that address this security vulnerability. CVE ID : CVE-2021-37731	https://www. arubanetwor ks.com/asset s/alert/ARUB A-PSA-2021- 016.txt	H-ARU-7240- 170921/340
7280					
Improper Limitation of a Pathname to a Restricted Directory ('Path Traversal')	07-Sep-21	7.2	A local path traversal vulnerability was discovered in Aruba SD-WAN Software and Gateways; Aruba Operating System Software version(s): Prior to 8.6.0.0- 2.2.0.4; Prior to 8.7.1.1, 8.6.0.7, 8.5.0.12, 8.3.0.16. Aruba has released patches for Aruba SD-WAN Software and Gateways and ArubaOS that address this security vulnerability. CVE ID : CVE-2021-37731	https://www. arubanetwor ks.com/asset s/alert/ARUB A-PSA-2021- 016.txt	H-ARU-7280- 170921/341

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
9004					L
Improper Limitation of a Pathname to a Restricted Directory ('Path Traversal')	07-Sep-21	7.2	A local path traversal vulnerability was discovered in Aruba SD-WAN Software and Gateways; Aruba Operating System Software version(s): Prior to 8.6.0.0- 2.2.0.4; Prior to 8.7.1.1, 8.6.0.7, 8.5.0.12, 8.3.0.16. Aruba has released patches for Aruba SD-WAN Software and Gateways and ArubaOS that address this security vulnerability. CVE ID : CVE-2021-37731	https://www. arubanetwor ks.com/asset s/alert/ARUB A-PSA-2021- 016.txt	H-ARU-9004- 170921/342
9004-lte					
Improper Limitation of a Pathname to a Restricted Directory ('Path Traversal')	07-Sep-21	7.2	A local path traversal vulnerability was discovered in Aruba SD-WAN Software and Gateways; Aruba Operating System Software version(s): Prior to 8.6.0.0- 2.2.0.4; Prior to 8.7.1.1, 8.6.0.7, 8.5.0.12, 8.3.0.16. Aruba has released patches for Aruba SD-WAN Software and Gateways and ArubaOS that address this security vulnerability. CVE ID : CVE-2021-37731	https://www. arubanetwor ks.com/asset s/alert/ARUB A-PSA-2021- 016.txt	H-ARU-9004- 170921/343
9012					<u> </u>
Improper Limitation of a Pathname to a Restricted Directory ('Path	07-Sep-21	7.2	A local path traversal vulnerability was discovered in Aruba SD-WAN Software and Gateways; Aruba Operating System Software version(s): Prior to 8.6.0.0- 2.2.0.4; Prior to 8.7.1.1,	https://www. arubanetwor ks.com/asset s/alert/ARUB A-PSA-2021- 016.txt	H-ARU-9012- 170921/344
CVSS Scoring Sc	ale 0-1	1-2	2-3 3-4 4-5 5-6 Page 130 of 1474	6-7 7-8	8-9 9-10

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Traversal') bluetrum			8.6.0.7, 8.5.0.12, 8.3.0.16. Aruba has released patches for Aruba SD-WAN Software and Gateways and ArubaOS that address this security vulnerability. CVE ID : CVE-2021-37731		
ab5301a					
N/A	07-Sep-21	3.3	The Bluetooth Classic implementation on Bluetrum AB5301A devices with unknown firmware versions does not properly handle the reception of oversized DM1 LMP packets while no other BT connections are active, allowing attackers in radio range to prevent new BT connections (disabling the AB5301A inquiry and page scan procedures) via a crafted LMP packet. The user needs to manually perform a power cycle (restart) of the device to restore BT connectivity. CVE ID : CVE-2021-34150	http://www. bluetrum.co m/product/a b5301a.html	H-BLU-AB53- 170921/345
ab5376t					
N/A	07-Sep-21	6.1	The Bluetooth Classic implementation on AB32VG1 devices does not properly handle the reception of continuous unsolicited LMP responses, allowing attackers in radio range to trigger a denial of service (either restart or deadlock the	http://www. bluetrum.co m/product/a b5376t.html, http://www. bluetrum.co m/product/b t8896a.html	H-BLU-AB53- 170921/346
CVSS Scoring Sc	ale 0-1	1-2	2-3 3-4 4-5 5-6 Dage 121 of 1474	6-7 7-8	8-9 9-10

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID	
			device) by flooding a device with LMP_AU_rand data.			
			CVE ID : CVE-2021-31610			
1:000			CVE ID : CVE-2021-31610			
bt8896a				Γ	Γ	
N/A	07-Sep-21	6.1	The Bluetooth Classic implementation on AB32VG1 devices does not properly handle the reception of continuous unsolicited LMP responses, allowing attackers in radio range to trigger a denial of service (either restart or deadlock the device) by flooding a device with LMP_AU_rand data.	http://www. bluetrum.co m/product/a b5376t.html, http://www. bluetrum.co m/product/b t8896a.html	H-BLU-BT88- 170921/347	
			CVE ID : CVE-2021-31610			
christiedigita	al					
dwu850-gs						
Improper Authenticati on	01-Sep-21	7.5	webctrl.cgi.elf on Christie Digital DWU850-GS V06.46 devices allows attackers to perform any desired action via a crafted query containing an unspecified Cookie header. Authentication bypass can be achieved by including an administrative cookie that the device does not validate. CVE ID : CVE-2021-40350	N/A	H-CHR- DWU8- 170921/348	
comprotech						
ip570	ip570					
Missing Authorizatio n	01-Sep-21	8.5	An issue was discovered on Compro IP70 2.08_7130218, IP570 2.08_7130520, IP60, and TN540 devices. /cgi- bin/support/killps.cgi	N/A	H-COM-IP57- 170921/349	
CVSS Scoring Sc	ale 0-1	1-2	2-3 3-4 4-5 5-6 Page 132 of 1474	6-7 7-8	8-9 9-10	

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			deletes all data from the device.		
			CVE ID : CVE-2021-40378		
Improper Privilege Managemen t	01-Sep-21	5	An issue was discovered on Compro IP70 2.08_7130218, IP570 2.08_7130520, IP60, and TN540 devices. rstp:///medias2 does not require authorization. CVE ID : CVE-2021-40379	N/A	H-COM-IP57- 170921/350
Improper Authenticati on	01-Sep-21	5	An issue was discovered on Compro IP70 2.08_7130218, IP570 2.08_7130520, IP60, and TN540 devices. cameralist.cgi and setcamera.cgi disclose credentials. CVE ID : CVE-2021-40380	N/A	H-COM-IP57- 170921/351
Improper Privilege Managemen t	01-Sep-21	5	An issue was discovered on Compro IP70 2.08_7130218, IP570 2.08_7130520, IP60, and TN540 devices. index_MJpeg.cgi allows video access. CVE ID : CVE-2021-40381	N/A	H-COM-IP57- 170921/352
Improper Privilege Managemen t	01-Sep-21	5	An issue was discovered on Compro IP70 2.08_7130218, IP570 2.08_7130520, IP60, and TN540 devices. mjpegStreamer.cgi allows video screenshot access. CVE ID : CVE-2021-40382	N/A	H-COM-IP57- 170921/353
ip60				L	I
Missing Authorizatio n	01-Sep-21	8.5	An issue was discovered on Compro IP70 2.08_7130218, IP570 2.08_7130520, IP60, and TN540 devices. /cgi-	N/A	H-COM-IP60- 170921/354
CVSS Scoring Sco	ale 0-1	1-2	2-3 3-4 4-5 5-6 Page 133 of 1474	6-7 7-8	8-9 9-10

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			bin/support/killps.cgi deletes all data from the device. CVE ID : CVE-2021-40378		
Improper Privilege Managemen t	01-Sep-21	5	An issue was discovered on Compro IP70 2.08_7130218, IP570 2.08_7130520, IP60, and TN540 devices. rstp:///medias2 does not require authorization. CVE ID : CVE-2021-40379	N/A	H-COM-IP60- 170921/355
Improper Authenticati on	01-Sep-21	5	An issue was discovered on Compro IP70 2.08_7130218, IP570 2.08_7130520, IP60, and TN540 devices. cameralist.cgi and setcamera.cgi disclose credentials. CVE ID : CVE-2021-40380	N/A	H-COM-IP60- 170921/356
Improper Privilege Managemen t	01-Sep-21	5	An issue was discovered on Compro IP70 2.08_7130218, IP570 2.08_7130520, IP60, and TN540 devices. index_MJpeg.cgi allows video access. CVE ID : CVE-2021-40381	N/A	H-COM-IP60- 170921/357
Improper Privilege Managemen t	01-Sep-21	5	An issue was discovered on Compro IP70 2.08_7130218, IP570 2.08_7130520, IP60, and TN540 devices. mjpegStreamer.cgi allows video screenshot access. CVE ID : CVE-2021-40382	N/A	H-COM-IP60- 170921/358
ip70	I			1	
Missing Authorizatio	01-Sep-21	8.5	An issue was discovered on Compro IP70 2.08_7130218, IP570 2.08_7130520, IP60,	N/A	H-COM-IP70- 170921/359
CVSS Scoring Sc	ale 0-1	1-2	2-3 3-4 4-5 5-6 Page 134 of 1474	6-7 7-8	8-9 9-10

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
n			and TN540 devices. /cgi- bin/support/killps.cgi deletes all data from the device.		
			CVE ID : CVE-2021-40378		
Improper Privilege Managemen t	01-Sep-21	5	An issue was discovered on Compro IP70 2.08_7130218, IP570 2.08_7130520, IP60, and TN540 devices. rstp:///medias2 does not require authorization. CVE ID : CVE-2021-40379	N/A	H-COM-IP70- 170921/360
Improper Authenticati on	01-Sep-21	5	An issue was discovered on Compro IP70 2.08_7130218, IP570 2.08_7130520, IP60, and TN540 devices. cameralist.cgi and setcamera.cgi disclose credentials. CVE ID : CVE-2021-40380	N/A	H-COM-IP70- 170921/361
Improper Privilege Managemen t	01-Sep-21	5	An issue was discovered on Compro IP70 2.08_7130218, IP570 2.08_7130520, IP60, and TN540 devices. index_MJpeg.cgi allows video access. CVE ID : CVE-2021-40381	N/A	H-COM-IP70- 170921/362
Improper Privilege Managemen t	01-Sep-21	5	An issue was discovered on Compro IP70 2.08_7130218, IP570 2.08_7130520, IP60, and TN540 devices. mjpegStreamer.cgi allows video screenshot access. CVE ID : CVE-2021-40382	N/A	H-COM-IP70- 170921/363
tn540					
Missing Authorizatio	01-Sep-21	8.5	An issue was discovered on Compro IP70 2.08_7130218,	N/A	H-COM-TN54-
CVSS Scoring Sc	ale 0-1	1-2	2-3 3-4 4-5 5-6 Page 135 of 1474	6-7 7-8	8-9 9-10

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
n			IP570 2.08_7130520, IP60, and TN540 devices. /cgi- bin/support/killps.cgi deletes all data from the device.		170921/364
			CVE ID : CVE-2021-40378		
Improper Privilege Managemen t	01-Sep-21	5	An issue was discovered on Compro IP70 2.08_7130218, IP570 2.08_7130520, IP60, and TN540 devices. rstp:///medias2 does not require authorization. CVE ID : CVE-2021-40379	N/A	H-COM-TN54- 170921/365
			An issue was discovered on		
Improper Authenticati on	01-Sep-21	5	Compro IP70 2.08_7130218, IP570 2.08_7130520, IP60, and TN540 devices. cameralist.cgi and setcamera.cgi disclose credentials.	N/A	H-COM-TN54- 170921/366
			CVE ID : CVE-2021-40380		
Improper Privilege Managemen t	01-Sep-21	5	An issue was discovered on Compro IP70 2.08_7130218, IP570 2.08_7130520, IP60, and TN540 devices. index_MJpeg.cgi allows video access.	N/A	H-COM-TN54- 170921/367
			CVE ID : CVE-2021-40381		
Improper Privilege Managemen t	01-Sep-21	5	An issue was discovered on Compro IP70 2.08_7130218, IP570 2.08_7130520, IP60, and TN540 devices. mjpegStreamer.cgi allows video screenshot access. CVE ID : CVE-2021-40382	N/A	H-COM-TN54- 170921/368
Cypress					

CVSS Scoring Scale

0-1

1-2

5-6

6-7

7-8

8-9

9-10

cyw20735b1	07-Sep-21		The Bluetooth Classic implementation in the Cypress WICED BT stack through 2.9.0 for CYW20735B1 devices does not properly handle the reception of LMP_max_slot	https://www. cypress.com/	
N/A 0	07-Sep-21		implementation in the Cypress WICED BT stack through 2.9.0 for CYW20735B1 devices does not properly handle the	cypress.com/	
		2.9	with an invalid Baseband packet type (and LT_ADDRESS and LT_ADDR) after completion of the LMP setup procedure, allowing attackers in radio range to trigger a denial of service (firmware crash) via a crafted LMP packet. CVE ID : CVE-2021-34145	documentatio n/datasheets /cyw20735b 1-single-chip- bluetooth- transceiver- wireless- input-devices	H-CYP-CYW2- 170921/369
N/A C	07-Sep-21	6.1	The Bluetooth Classic implementation in the Cypress CYW920735Q60EVB does not properly handle the reception of continuous unsolicited LMP responses, allowing attackers in radio range to trigger a denial of service and restart (crash) of the device by flooding it with LMP_AU_Rand packets after the paging procedure. CVE ID : CVE-2021-34146	https://www. cypress.com/ documentatio n/datasheets /cyw20735b 1-single-chip- bluetooth- transceiver- wireless- input-devices	H-CYP-CYW2- 170921/370
N/A (07-Sep-21	6.1	The Bluetooth Classic implementation in the Cypress WICED BT stack through 2.9.0 for CYW20735B1 does not properly handle the reception of a malformed LMP timing accuracy	https://www. cypress.com/ documentatio n/datasheets /cyw20735b 1-single-chip- bluetooth- transceiver-	H-CYP-CYW2- 170921/371

	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID		
			response followed by multiple reconnections to the link slave, allowing attackers to exhaust device BT resources and eventually trigger a crash via multiple attempts of sending a crafted LMP timing accuracy response followed by a sudden reconnection with a random BDAddress. CVE ID : CVE-2021-34147	wireless- input-devices			
			The Bluetooth Classic				
N/A	07-Sep-21	6.1	implementation in the Cypress WICED BT stack through 2.9.0 for CYW20735B1 devices does not properly handle the reception of LMP_max_slot with a greater ACL Length after completion of the LMP setup procedure, allowing attackers in radio range to trigger a denial of service (firmware crash) via a crafted LMP packet.	https://www. cypress.com/ documentatio n/datasheets /cyw20735b 1-single-chip- bluetooth- transceiver- wireless- input-devices	H-CYP-CYW2- 170921/372		
			CVE ID : CVE-2021-34148				
cyw920735q60evb-01							
N/A	07-Sep-21	6.1	The Bluetooth Classic implementation in the Cypress CYW920735Q60EVB does not properly handle the reception of continuous unsolicited LMP responses, allowing attackers in radio range to trigger a denial of service and restart (crash) of the device by flooding it with LMP_AU_Rand packets after	https://www. cypress.com/ documentatio n/datasheets /cyw20735b 1-single-chip- bluetooth- transceiver- wireless- input-devices	H-CYP-CYW9- 170921/373		

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID		
			the paging procedure.				
			CVE ID : CVE-2021-34146				
espressif	·						
esp32	esp32						
Out-of- bounds Write	07-Sep-21	3.3	The Bluetooth Classic implementation in Espressif ESP-IDF 4.4 and earlier does not properly handle the reception of multiple LMP IO Capability Request packets during the pairing process, allowing attackers in radio range to trigger memory corruption (and consequently a crash) in ESP32 via a replayed (duplicated) LMP packet. CVE ID : CVE-2021-28136	https://www. espressif.com /en/products /socs/esp32	H-ESP-ESP3- 170921/374		
N/A	07-Sep-21	8.3	The Bluetooth Classic implementation in Espressif ESP-IDF 4.4 and earlier does not properly restrict the Feature Page upon reception of an LMP Feature Response Extended packet, allowing attackers in radio range to trigger arbitrary code execution in ESP32 via a crafted Extended Features bitfield payload. CVE ID : CVE-2021-28139	https://www. espressif.com /en/products /socs/esp32	H-ESP-ESP3- 170921/375		
jbl	·						
tune500bt							
N/A	07-Sep-21	6.1	The Bluetooth Classic implementation on JBL TUNE500BT devices does not properly handle the	https://www. jbl.com.sg/ov er-ear- headphones/J	H-JBL-TUNE- 170921/376		
CVSS Scoring S	cale 0-1	1-2	2-3 3-4 4-5 5-6	6-7 7-8	8-9 9-10		

Improper Input Validation01-Sep-21Sep-21Wireless devices via allowing attackers to the systog configuration form. An authenticated remote attacker could remote attacker could re	Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID	
experia_wifiexperia_wifiWireless devices running certain Arcadyan-derived firmware (such as KPN Experia WiFi 1.00.15) do not properly sanitise user input to the syslog configuration form. An authenticated remote attacker could leverage this to alter the device configuration and achieve remote code execution. This can be exploited in conjunction with CVE-2021-20090. CVE ID : CVE-2021-38703https://www. ktps://www. lr0921/377mimiN/A07-Sep-216.1The Bluetooth Classic implementation on AB32VG1 devices does not properly handle the reception of continuous unsolicited LMP response, allowing attackers in radio range to trigger a denial of service (eitherhttp://www. bluetrum.co m/product/bN/A07-Sep-216.1The Bluetooth Classic implementation on AB32VG1 devices does not properly handle the reception of continuous unsolicited LMP responses, allowing attackers in radio range to trigger a denial of service (eitherhttp://www. bluetrum.co m/product/b				unsolicited LMP responses, allowing attackers in radio range to trigger a denial of service and shutdown a device by flooding the target device with LMP Feature Response data.			
Improper Input Validation01-Sep-219Wireless devices running certain Arcadyan-derived firmware (such as KPN Experia WiFi 1.00.15) do not properly sanitise user input to the syslog configuration form. An authenticated remote attacker could leverage this to alter the device configuration and achieve remote code execution. This can be exploited in conjunction with CVE-2021-20090. CVE ID : CVE-2021-38703https://www. kpnwebshop. com/modems 	-						
Improper Input Validation01-Sep-219certain Arcadyan-derived firmware (such as KPN Experia WiFi 1.00.15) do not properly sanitise user input to the syslog configuration form. An authenticated leverage this to alter the device configuration and achieve remote code execution. This can be exploited in conjunction with CVE-2021-20090. CVE ID : CVE-2021-38703https://www. http://www. http://www. http://www. bluetrum.comiM/A07-Sep-216.1The Bluetooth Classic implementation on AB32VG1 continuous unsolicited LMP handle the reception of in radio range to trigger a denial of service (eitherhttp://www. bluetrum.co m/product/bH-MI-MI_T- 170921/378	experia_wifi						
mi_true_wireless_earbuds_basic_2mi_true_wireless_earbuds_basic_2N/AFile Bluetooth Classic implementation on AB32VG1N/AN/A07-Sep-21Andle the reception of continuous unsolicited LMP responses, allowing attackers in radio range to trigger a denial of service (eitherMather H-MI-MI_T- m/product/bMather H-MI-MI_T- m/product/bMather H-MI-MI_T- m/product/bMather H-MI-MI_T- mather H-MI-MI_T- mather H-MI-MI_T- http://www.Mather H-MI-MI_T- mather H-MI-MI_T- mather H-MI-MI_T- mather H-MI-MI_T- http://www.Mather H-MI-MI_T- http://www.Mather H-MI-MI_T- mather H-MI-MI_T- http://www.Mather H-MI-MI_T- mather H-MI-MI_T- http://www.Mather H-MI-MI_T- mather H-MI-MI_T- http://www.Mather H-MI-MI_T- http://www.Mather H-MI-MI_T- http://www.Mather H-MI-MI_T- http://www.Mather H-MI-MI_T- http://www.Mather H-MI-MI_T- http://www. <t< td=""><td>Input</td><td>01-Sep-21</td><td>9</td><td>certain Arcadyan-derived firmware (such as KPN Experia WiFi 1.00.15) do not properly sanitise user input to the syslog configuration form. An authenticated remote attacker could leverage this to alter the device configuration and achieve remote code execution. This can be exploited in conjunction with CVE-2021-20090.</td><td>kpnwebshop. com/modems - routers/prod ucten/experi</td><td>H-KPN-EXPE- 170921/377</td></t<>	Input	01-Sep-21	9	certain Arcadyan-derived firmware (such as KPN Experia WiFi 1.00.15) do not properly sanitise user input to the syslog configuration form. An authenticated remote attacker could leverage this to alter the device configuration and achieve remote code execution. This can be exploited in conjunction with CVE-2021-20090.	kpnwebshop. com/modems - routers/prod ucten/experi	H-KPN-EXPE- 170921/377	
N/A 07-Sep-21 6.1 The Bluetooth Classic implementation on AB32VG1 http://www. bluetrum.co handle the reception of m/product/a continuous unsolicited LMP b5376t.html, H-MI-MI_T- responses, allowing attackers in radio range to trigger a denial of service (either m/product/b)	mi						
N/A 07-Sep-21 6.1 implementation on AB32VG1 http://www. bluetrum.co handle the reception of m/product/a continuous unsolicited LMP b5376t.html, H-MI-MI_T- responses, allowing attackers in radio range to trigger a denial of service (either m/product/b	mi_true_wireless_earbuds_basic_2						
device) by flooding a device	N/A	07-Sep-21	6.1	implementation on AB32VG1 devices does not properly handle the reception of continuous unsolicited LMP responses, allowing attackers in radio range to trigger a denial of service (either restart or deadlock the	bluetrum.co m/product/a b5376t.html, http://www. bluetrum.co m/product/b	_	

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			with LMP_AU_rand data.		
			CVE ID : CVE-2021-31610		
Moxa					
oncell_g3470)a-lte-eu				
Improper Neutralizati on of Input During Web Page Generation ('Cross-site Scripting')	07-Sep-21	4.3	Certain MOXA devices allow reflected XSS via the Config Import menu. This affects WAC-2004 1.7, WAC-1001 2.1, WAC-1001-T 2.1, OnCell G3470A-LTE-EU 1.7, OnCell G3470A-LTE-EU-T 1.7, TAP- 323-EU-CT-T 1.3, TAP-323- US-CT-T 1.3, TAP-323-JP-CT- T 1.3, WDR-3124A-EU 2.3, WDR-3124A-EU-T 2.3, WDR- 3124A-US 2.3, and WDR- 3124A-US-T 2.3.	N/A	H-MOX-ONCE- 170921/379
			CVE ID : CVE-2021-39278		
Improper Neutralizati on of Special Elements used in an OS Command ('OS Command Injection')	07-Sep-21	9	Certain MOXA devices allow Authenticated Command Injection via /forms/web_importTFTP. This affects WAC-2004 1.7, WAC-1001 2.1, WAC-1001-T 2.1, OnCell G3470A-LTE-EU 1.7, OnCell G3470A-LTE-EU T 1.7, TAP-323-EU-CT-T 1.3, TAP-323-US-CT-T 1.3, TAP- 323-JP-CT-T 1.3, WDR- 3124A-EU 2.3, WDR-3124A- EU-T 2.3, WDR-3124A-US 2.3, and WDR-3124A-US-T 2.3. CVE ID : CVE-2021-39279	https://www. moxa.com	H-MOX-ONCE- 170921/380
oncell_g3470)a-lte-eu-t				
Improper Neutralizati	07-Sep-21	4.3	Certain MOXA devices allow reflected XSS via the Config	N/A	H-MOX-ONCE- 170921/381
CVSS Scoring Sc	ale 0-1	1-2	2-3 3-4 4-5 5-6 Page 141 of 1474	6-7 7-8	8-9 <mark>9-10</mark>

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID			
on of Input During Web Page Generation ('Cross-site Scripting')			Import menu. This affects WAC-2004 1.7, WAC-1001 2.1, WAC-1001-T 2.1, OnCell G3470A-LTE-EU 1.7, OnCell G3470A-LTE-EU-T 1.7, TAP- 323-EU-CT-T 1.3, TAP-323- US-CT-T 1.3, TAP-323-JP-CT- T 1.3, WDR-3124A-EU 2.3, WDR-3124A-EU-T 2.3, WDR- 3124A-US 2.3, and WDR- 3124A-US-T 2.3.					
			CVE ID : CVE-2021-39278					
Improper Neutralizati on of Special Elements used in an OS Command ('OS Command Injection')	07-Sep-21	9	Certain MOXA devices allow Authenticated Command Injection via /forms/web_importTFTP. This affects WAC-2004 1.7, WAC-1001 2.1, WAC-1001-T 2.1, OnCell G3470A-LTE-EU 1.7, OnCell G3470A-LTE-EU T 1.7, TAP-323-EU-CT-T 1.3, TAP-323-US-CT-T 1.3, TAP- 323-JP-CT-T 1.3, WDR- 3124A-EU 2.3, WDR-3124A- EU-T 2.3, WDR-3124A-US 2.3, and WDR-3124A-US-T 2.3. CVE ID : CVE-2021-39279	https://www. moxa.com	H-MOX-ONCE- 170921/382			
tap-323-eu-c	tap-323-eu-ct-t							
Improper Neutralizati on of Input During Web Page Generation ('Cross-site Scripting')	07-Sep-21	4.3	Certain MOXA devices allow reflected XSS via the Config Import menu. This affects WAC-2004 1.7, WAC-1001 2.1, WAC-1001-T 2.1, OnCell G3470A-LTE-EU 1.7, OnCell G3470A-LTE-EU-T 1.7, TAP- 323-EU-CT-T 1.3, TAP-323- US-CT-T 1.3, TAP-323-JP-CT- T 1.3, WDR-3124A-EU 2.3,	N/A	H-MOX-TAP 170921/383			
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
			WDR-3124A-EU-T 2.3, WDR- 3124A-US 2.3, and WDR- 3124A-US-T 2.3.		
			CVE ID : CVE-2021-39278		
Improper Neutralizati on of Special Elements used in an OS Command ('OS Command Injection')	07-Sep-21	9	Certain MOXA devices allow Authenticated Command Injection via /forms/web_importTFTP. This affects WAC-2004 1.7, WAC-1001 2.1, WAC-1001-T 2.1, OnCell G3470A-LTE-EU 1.7, OnCell G3470A-LTE-EU T 1.7, TAP-323-EU-CT-T 1.3, TAP-323-US-CT-T 1.3, TAP- 323-JP-CT-T 1.3, WDR- 3124A-EU 2.3, WDR-3124A- EU-T 2.3, WDR-3124A-US 2.3, and WDR-3124A-US-T 2.3. CVE ID : CVE-2021-39279	https://www. moxa.com	H-MOX-TAP 170921/384
tap-323-jp-ct	t-t				
Improper Neutralizati on of Input During Web Page Generation ('Cross-site Scripting')	07-Sep-21	4.3	Certain MOXA devices allow reflected XSS via the Config Import menu. This affects WAC-2004 1.7, WAC-1001 2.1, WAC-1001-T 2.1, OnCell G3470A-LTE-EU 1.7, OnCell G3470A-LTE-EU-T 1.7, TAP- 323-EU-CT-T 1.3, TAP-323- US-CT-T 1.3, TAP-323-JP-CT- T 1.3, WDR-3124A-EU 2.3, WDR-3124A-EU-T 2.3, WDR- 3124A-US 2.3, and WDR- 3124A-US-T 2.3. CVE ID : CVE-2021-39278	N/A	H-MOX-TAP 170921/385
Improper Neutralizati on of Special	07-Sep-21	9	Certain MOXA devices allow Authenticated Command Injection via	https://www. moxa.com	H-MOX-TAP 170921/386

Page 144 of 1474

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			3124A-EU 2.3, WDR-3124A- EU-T 2.3, WDR-3124A-US 2.3, and WDR-3124A-US-T 2.3. CVE ID : CVE-2021-39279		
wac-1001					<u> </u>
Improper Neutralizati on of Input During Web Page Generation ('Cross-site Scripting')	07-Sep-21	4.3	Certain MOXA devices allow reflected XSS via the Config Import menu. This affects WAC-2004 1.7, WAC-1001 2.1, WAC-1001-T 2.1, OnCell G3470A-LTE-EU 1.7, OnCell G3470A-LTE-EU-T 1.7, TAP- 323-EU-CT-T 1.3, TAP-323- US-CT-T 1.3, TAP-323-JP-CT- T 1.3, WDR-3124A-EU 2.3, WDR-3124A-EU-T 2.3, WDR- 3124A-US 2.3, and WDR- 3124A-US-T 2.3. CVE ID : CVE-2021-39278	N/A	H-MOX-WAC 170921/389
Improper Neutralizati on of Special Elements used in an OS Command ('OS Command Injection')	07-Sep-21	9	Certain MOXA devices allow Authenticated Command Injection via /forms/web_importTFTP. This affects WAC-2004 1.7, WAC-1001 2.1, WAC-1001-T 2.1, OnCell G3470A-LTE-EU 1.7, OnCell G3470A-LTE-EU- T 1.7, TAP-323-EU-CT-T 1.3, TAP-323-US-CT-T 1.3, TAP- 323-JP-CT-T 1.3, WDR- 3124A-EU 2.3, WDR-3124A- EU-T 2.3, WDR-3124A-US 2.3, and WDR-3124A-US-T 2.3. CVE ID : CVE-2021-39279	https://www. moxa.com	H-MOX-WAC 170921/390
wac-1001-t					

0-1

1-2

2-3 3-4

4-5

5-6

6-7

7-8

8-9

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Improper Neutralizati on of Input During Web Page Generation ('Cross-site Scripting')	07-Sep-21	4.3	Certain MOXA devices allow reflected XSS via the Config Import menu. This affects WAC-2004 1.7, WAC-1001 2.1, WAC-1001-T 2.1, OnCell G3470A-LTE-EU 1.7, OnCell G3470A-LTE-EU-T 1.7, TAP- 323-EU-CT-T 1.3, TAP-323- US-CT-T 1.3, TAP-323-JP-CT- T 1.3, WDR-3124A-EU 2.3, WDR-3124A-EU-T 2.3, WDR- 3124A-US 2.3, and WDR- 3124A-US-T 2.3. CVE ID : CVE-2021-39278	N/A	H-MOX-WAC 170921/391
Improper Neutralizati on of Special Elements used in an OS Command ('OS Command Injection')	07-Sep-21	9	Certain MOXA devices allow Authenticated Command Injection via /forms/web_importTFTP. This affects WAC-2004 1.7, WAC-1001 2.1, WAC-1001-T 2.1, OnCell G3470A-LTE-EU 1.7, OnCell G3470A-LTE-EU T 1.7, TAP-323-EU-CT-T 1.3, TAP-323-US-CT-T 1.3, TAP- 323-JP-CT-T 1.3, WDR- 3124A-EU 2.3, WDR-3124A- EU-T 2.3, WDR-3124A-US 2.3, and WDR-3124A-US-T 2.3. CVE ID : CVE-2021-39279	https://www. moxa.com	H-MOX-WAC 170921/392
wac-2004					
Improper Neutralizati on of Input During Web Page Generation ('Cross-site	07-Sep-21	4.3	Certain MOXA devices allow reflected XSS via the Config Import menu. This affects WAC-2004 1.7, WAC-1001 2.1, WAC-1001-T 2.1, OnCell G3470A-LTE-EU 1.7, OnCell G3470A-LTE-EU-T 1.7, TAP- 323-EU-CT-T 1.3, TAP-323-	N/A	H-MOX-WAC 170921/393
CVSS Scoring Sc	ale 0-1	1-2	2-3 3-4 4-5 5-6 Page 146 of 1474	6-7 7-8	8-9 9-10

Page 146 of 1474

Scripting')US-CT-T 1.3, TAP-323-IP-CT- T 1.3, WDR-3124A-EU 2.3, WDR-3124A-EU 2.3, and WDR- 3124A-US-T 2.3.Here is the second	Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Improper Neutralizati on of Special Elements used in an OS Command (Injection')Certain MOXA devices allow Authenticated Command Injection via /forms/web_importTFTP. This affects WAC-2004 1.7, WAC-1001 2.1, WAC-1001-T 2.1, OnCell G3470A-LTE-EU- 1.7, OnCell G3470A-LTE-EU- T 1.7, TAP-323-EU-CT-T 1.3, TAP- 323-IP-CT-T 1.3, WDR- 3124A-EU 2.3, WDR-3124A- EU-T 2.3, WDR-3124A-US-T 2.3.Https://www. moxa.comH-MOX-WAC- I70921/394wdr-3124a-euVCertain MOXA devices allow reflected XSS via the Config Improper Neutralizati on of Input During Web Page Generation ('Cross-site Scripting')07-Sep-214.3Certain MOXA devices allow reflected XSS via the Config G3470A-LTE-EU 1.7, OnCell G3470A-LTE-EU 1.7, ONCell <br< td=""><td>Scripting')</td><td></td><td></td><td>T 1.3, WDR-3124A-EU 2.3, WDR-3124A-EU-T 2.3, WDR- 3124A-US 2.3, and WDR-</td><td></td><td></td></br<>	Scripting')			T 1.3, WDR-3124A-EU 2.3, WDR-3124A-EU-T 2.3, WDR- 3124A-US 2.3, and WDR-		
Improper Neutralizati on of Special Elements used in an (OS Command 				CVE ID : CVE-2021-39278		
Improper Neutralizati on of Input During Web Page Generation ('Cross-site Scripting')07-Sep-21Certain MOXA devices allow reflected XSS via the Config Import menu. This affects WAC-2004 1.7, WAC-1001 2.1, WAC-1001-T 2.1, OnCell G3470A-LTE-EU 1.7, OnCell G3470A-LTE-EU-T 1.7, TAP- 323-EU-CT-T 1.3, TAP-323- US-CT-T 1.3, TAP-323-JP-CT- T 1.3, WDR-3124A-EU 2.3, WDR-3124A-EU 2.3, and WDR- 3124A-US-T 2.3.H-MOX-WDR- H-MOX-WDR- 170921/395	Neutralizati on of Special Elements used in an OS Command ('OS Command	07-Sep-21	9	Authenticated Command Injection via /forms/web_importTFTP. This affects WAC-2004 1.7, WAC-1001 2.1, WAC-1001-T 2.1, OnCell G3470A-LTE-EU 1.7, OnCell G3470A-LTE-EU- T 1.7, TAP-323-EU-CT-T 1.3, TAP-323-US-CT-T 1.3, TAP- 323-JP-CT-T 1.3, WDR- 3124A-EU 2.3, WDR-3124A- EU-T 2.3, WDR-3124A-US 2.3, and WDR-3124A-US-T 2.3.		H-MOX-WAC 170921/394
Improper Neutralizati on of Input During Web Page Generation ('Cross-site Scripting')07-Sep-214.3reflected XSS via the Config Import menu. This affects WAC-2004 1.7, WAC-1001 2.1, WAC-1001-T 2.1, OnCell G3470A-LTE-EU 1.7, OnCell G3470A-LTE-EU-T 1.7, TAP- 323-EU-CT-T 1.3, TAP-323- US-CT-T 1.3, TAP-323-JP-CT- T 1.3, WDR-3124A-EU 2.3, WDR-3124A-EU 2.3, and WDR- 3124A-US-T 2.3.H-MOX-WDR- H-MOX-WDR- Page H-MOX-WDR- 	wdr-3124a-e	eu				
	Neutralizati on of Input During Web Page Generation ('Cross-site	07-Sep-21	4.3	reflected XSS via the Config Import menu. This affects WAC-2004 1.7, WAC-1001 2.1, WAC-1001-T 2.1, OnCell G3470A-LTE-EU 1.7, OnCell G3470A-LTE-EU-T 1.7, TAP- 323-EU-CT-T 1.3, TAP-323- US-CT-T 1.3, TAP-323-JP-CT- T 1.3, WDR-3124A-EU 2.3, WDR-3124A-EU-T 2.3, WDR- 3124A-US 2.3, and WDR- 3124A-US-T 2.3.	N/A	
Improper07-Sep-219Certain MOXA devices allowhttps://www.H-MOX-WDR-	Improper	07-Sep-21	9	Certain MOXA devices allow	https://www.	H-MOX-WDR-

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Neutralizati on of Special Elements used in an OS Command ('OS Command Injection')			Authenticated Command Injection via /forms/web_importTFTP. This affects WAC-2004 1.7, WAC-1001 2.1, WAC-1001-T 2.1, OnCell G3470A-LTE-EU 1.7, OnCell G3470A-LTE-EU T 1.7, TAP-323-EU-CT-T 1.3, TAP-323-US-CT-T 1.3, TAP- 323-JP-CT-T 1.3, WDR- 3124A-EU 2.3, WDR-3124A- EU-T 2.3, WDR-3124A-US 2.3, and WDR-3124A-US-T 2.3.	moxa.com	-170921/396
wdr-3124a-e			CVE ID : CVE-2021-39279		
Improper Neutralizati on of Input During Web Page Generation ('Cross-site Scripting')	07-Sep-21	4.3	Certain MOXA devices allow reflected XSS via the Config Import menu. This affects WAC-2004 1.7, WAC-1001 2.1, WAC-1001-T 2.1, OnCell G3470A-LTE-EU 1.7, OnCell G3470A-LTE-EU-T 1.7, TAP- 323-EU-CT-T 1.3, TAP-323- US-CT-T 1.3, TAP-323-JP-CT- T 1.3, WDR-3124A-EU 2.3, WDR-3124A-EU-T 2.3, WDR- 3124A-US 2.3, and WDR- 3124A-US-T 2.3. CVE ID : CVE-2021-39278	N/A	H-MOX-WDR- -170921/397
Improper Neutralizati on of Special Elements used in an OS Command ('OS Command	07-Sep-21	9	Certain MOXA devices allow Authenticated Command Injection via /forms/web_importTFTP. This affects WAC-2004 1.7, WAC-1001 2.1, WAC-1001-T 2.1, OnCell G3470A-LTE-EU 1.7, OnCell G3470A-LTE-EU- T 1.7, TAP-323-EU-CT-T 1.3,	https://www. moxa.com	H-MOX-WDR- -170921/398
CVSS Scoring Sc	ale 0-1	1-2	2-3 3-4 4-5 5-6	6-7 7-8	8-9 9-10

Page 148 of 1474

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Injection')			TAP-323-US-CT-T 1.3, TAP- 323-JP-CT-T 1.3, WDR- 3124A-EU 2.3, WDR-3124A- EU-T 2.3, WDR-3124A-US 2.3, and WDR-3124A-US-T 2.3. CVE ID : CVE-2021-39279		
wdr-3124a-u	S				
Improper Neutralizati on of Input During Web Page Generation ('Cross-site Scripting')	07-Sep-21	4.3	Certain MOXA devices allow reflected XSS via the Config Import menu. This affects WAC-2004 1.7, WAC-1001 2.1, WAC-1001-T 2.1, OnCell G3470A-LTE-EU 1.7, OnCell G3470A-LTE-EU-T 1.7, TAP- 323-EU-CT-T 1.3, TAP-323- US-CT-T 1.3, TAP-323-JP-CT- T 1.3, WDR-3124A-EU 2.3, WDR-3124A-EU-T 2.3, WDR- 3124A-US 2.3, and WDR- 3124A-US-T 2.3. CVE ID : CVE-2021-39278	N/A	H-MOX-WDR- -170921/399
Improper Neutralizati on of Special Elements used in an OS Command ('OS Command Injection')	07-Sep-21	9	Certain MOXA devices allow Authenticated Command Injection via /forms/web_importTFTP. This affects WAC-2004 1.7, WAC-1001 2.1, WAC-1001-T 2.1, OnCell G3470A-LTE-EU 1.7, OnCell G3470A-LTE-EU- T 1.7, TAP-323-EU-CT-T 1.3, TAP-323-US-CT-T 1.3, TAP- 323-JP-CT-T 1.3, WDR- 3124A-EU 2.3, WDR-3124A- EU-T 2.3, WDR-3124A-US 2.3, and WDR-3124A-US-T 2.3. CVE ID : CVE-2021-39279	https://www. moxa.com	H-MOX-WDR- -170921/400

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
wdr-3124a-u	ls-t				
Improper Neutralizati on of Input During Web Page Generation ('Cross-site Scripting')	07-Sep-21	4.3	Certain MOXA devices allow reflected XSS via the Config Import menu. This affects WAC-2004 1.7, WAC-1001 2.1, WAC-1001-T 2.1, OnCell G3470A-LTE-EU 1.7, OnCell G3470A-LTE-EU-T 1.7, TAP- 323-EU-CT-T 1.3, TAP-323- US-CT-T 1.3, TAP-323-JP-CT- T 1.3, WDR-3124A-EU 2.3, WDR-3124A-EU-T 2.3, WDR- 3124A-US 2.3, and WDR- 3124A-US-T 2.3. CVE ID : CVE-2021-39278	N/A	H-MOX-WDR- -170921/401
Improper Neutralizati on of Special Elements used in an OS Command ('OS Command Injection')	07-Sep-21	9	Certain MOXA devices allow Authenticated Command Injection via /forms/web_importTFTP. This affects WAC-2004 1.7, WAC-1001 2.1, WAC-1001-T 2.1, OnCell G3470A-LTE-EU 1.7, OnCell G3470A-LTE-EU T 1.7, TAP-323-EU-CT-T 1.3, TAP-323-US-CT-T 1.3, TAP- 323-JP-CT-T 1.3, WDR- 3124A-EU 2.3, WDR-3124A- EU-T 2.3, WDR-3124A-US 2.3, and WDR-3124A-US-T 2.3. CVE ID : CVE-2021-39279	https://www. moxa.com	H-MOX-WDR- -170921/402
oculus					
rift					
Buffer Copy without Checking Size of Input ('Classic	08-Sep-21	9.3	Medium by Adobe version 2.4.5.331 (and earlier) is affected by a buffer overflow vulnerability when parsing a crafted file. An	https://helpx .adobe.com/s ecurity/prod ucts/medium /apsb21-	H-OCU-RIFT- 170921/403
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 & CVE ID	Patch	NCIIPC ID
Buffer Overflow')			unauthenticated attacker could leverage this vulnerability to achieve remote 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-2021-28580	34.html	
rift_s	I			I	I
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	08-Sep-21	9.3	Medium by Adobe version 2.4.5.331 (and earlier) is affected by a buffer overflow vulnerability when parsing a crafted file. An unauthenticated attacker could leverage this vulnerability to achieve remote 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-2021-28580	https://helpx .adobe.com/s ecurity/prod ucts/medium /apsb21- 34.html	H-OCU-RIFT- 170921/404
touch	L				L
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	08-Sep-21	9.3	Medium by Adobe version 2.4.5.331 (and earlier) is affected by a buffer overflow vulnerability when parsing a crafted file. An unauthenticated attacker could leverage this vulnerability to achieve remote code execution in the context of the current user. Exploitation of this issue	https://helpx .adobe.com/s ecurity/prod ucts/medium /apsb21- 34.html	H-OCU-TOUC- 170921/405

CVSS Scoring Scale	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10
			Р	age 151 c	of 1474					

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			requires user interaction in that a victim must open a malicious file.		
			CVE ID : CVE-2021-28580		
Qualcomm					
apq8009				1	
Exposure of Resource to Wrong Sphere	08-Sep-21	2.1	Child process can leak information from parent process due to numeric pids are getting compared and these pid can be reused in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables CVE ID : CVE-2021-1904	https://www. qualcomm.co m/company/ product- security/bull etins/august- 2021-bulletin	H-QUA-APQ8- 170921/406
Loop with Unreachable Exit Condition ('Infinite Loop')	08-Sep-21	5	Loop with unreachable exit condition may occur due to improper handling of unsupported input in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Voice & Music, Snapdragon Wearables CVE ID : CVE-2021-1914	https://www. qualcomm.co m/company/ product- security/bull etins/august- 2021-bulletin	H-QUA-APQ8- 170921/407
Out-of- bounds Write	08-Sep-21	10	Possible buffer underflow due to lack of check for negative indices values when processing user provided input in Snapdragon Auto,	https://www. qualcomm.co m/company/ product- security/bull	H-QUA-APQ8- 170921/408

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Voice & Music, Snapdragon Wearables	etins/august- 2021-bulletin	
			CVE ID : CVE-2021-1916		
Integer Underflow (Wrap or Wraparoun d)	08-Sep-21	10	Integer underflow can occur when the RTCP length is lesser than than the actual blocks present in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Voice & Music, Snapdragon Wearables	https://www. qualcomm.co m/company/ product- security/bull etins/august- 2021-bulletin	H-QUA-APQ8- 170921/409
			CVE ID : CVE-2021-1919		
Integer Underflow (Wrap or Wraparoun d)	08-Sep-21	10	Integer underflow can occur due to improper handling of incoming RTCP packets in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Voice & Music, Snapdragon Wearables	https://www. qualcomm.co m/company/ product- security/bull etins/august- 2021-bulletin	H-QUA-APQ8- 170921/410
			CVE ID : CVE-2021-1920		
Out-of- bounds Read	08-Sep-21	3.6	Buffer over read could occur due to incorrect check of buffer size while flashing emmc devices in Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon	https://www. qualcomm.co m/company/ product- security/bull etins/august-	H-QUA-APQ8- 170921/411

CV33 SCOULD SCALE	ring Scale	Scoring Scale	CVSS
-------------------	------------	---------------	------

0-1

1-2

5-6

6-7

7-8

8-9

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking	2021-bulletin	
			CVE ID : CVE-2021-1928		
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	08-Sep-21	10	Possible buffer overflow due to improper validation of device types during P2P search in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Woice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking CVE ID : CVE-2021-1972	https://www. qualcomm.co m/company/ product- security/bull etins/august- 2021-bulletin	H-QUA-APQ8- 170921/412
apq8009w					
Exposure of Resource to Wrong Sphere	08-Sep-21	2.1	Child process can leak information from parent process due to numeric pids are getting compared and these pid can be reused in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables	https://www. qualcomm.co m/company/ product- security/bull etins/august- 2021-bulletin	H-QUA-APQ8- 170921/413
			CVE ID : CVE-2021-1904		

		condition may occur due to	gualcomm co	170021 / 11 4
		improper handling of unsupported input in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Voice & Music, Snapdragon Wearables	qualcomm.co m/company/ product- security/bull etins/august- 2021-bulletin	170921/414
		CVE ID : CVE-2021-1914		
08-Sep-21	10	Possible buffer underflow due to lack of check for negative indices values when processing user provided input in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Voice & Music, Snapdragon Wearables	https://www. qualcomm.co m/company/ product- security/bull etins/august- 2021-bulletin	H-QUA-APQ8- 170921/415
		CVE ID : CVE-2021-1916		
08-Sep-21	10	Integer underflow can occur when the RTCP length is lesser than than the actual blocks present in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Voice & Music, Snapdragon Wearables CVE ID : CVE-2021-1919	https://www. qualcomm.co m/company/ product- security/bull etins/august- 2021-bulletin	H-QUA-APQ8- 170921/416
08-Sep-21	10	Integer underflow can occur	https://www.	H-QUA-APQ8-
•	08-Sep-21	08-Sep-21 10	08-Sep-2110Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Industrial IOT, Snapdragon IOT, Snapdragon Voice & Music, Snapdragon Wearables08-Sep-2110Possible buffer underflow due to lack of check for negative indices values when processing user provided input in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer IOT, Snapdragon Consumer IOT, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Industrial IOT, Snapdragon IOT, Snapdragon Voice & Music, Snapdragon Outragon Connectivity, Snapdragon Connectivity, Snapdragon Connectivity, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Consumer IOT, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Industrial IOT, Snapdragon Consumer IOT, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snap	Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Industrial IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Wearablessecurity/bull etins/august- 2021-bulletin08-Sep-2110Possible buffer underflow due to lack of check for negative indices values when processing user provided input in Snapdragon Auto, Snapdragon Compute, Snapdragon Compute, Snapdragon Industrial IOT, Snapdragon Compute, Snapdragon Compute, Snapdragon IoT, Snapdragon Voice & Music, Snapdragon Muto, Snapdragon Compute, Snapdragon IoT, Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Connectivity, Snapdragon IoT, Snapdragon Auto, Snapdragon Compute, Snapdragon IoT, Snapdragon Auto, Snapdragon Compute, Snapdragon IoT, Snapdragon Noice & Music, Snapdragon Voice & Music, Snapdragon <br< td=""></br<>

Page 155 of 1474

Underflow (Wrap or Wraparoun d)Integration (Wrap or Wraparoun d)Integration (Wrap or Wraparoun d)Integration (Mraparoun d)Integration (Mraparoun d)Integration (Mraparoun d)Integration (Mraparoun (Mraparoun d)Integration (Mraparoun (Mraparoun d)Integration (Mraparoun (Mraparoun d)Integration (Mraparoun (Mraparadoun (Mraparoun	Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')Image: Comparison of the comparison o	(Wrap or Wraparoun			incoming RTCP packets in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Voice & Music, Snapdragon Wearables	m/company/ product- security/bull etins/august-	170921/417
Exposure of Resource to Sphere08-Sep-21East Napple Child process can leak information from parent process due to numeric pids these pid can be reused in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile,https://www. qualcomm.co m/company/ product- security/bull etins/august- 2021-bulletinH-QUA-APQ8- 10921/419	without Checking Size of Input ('Classic Buffer	08-Sep-21	10	to improper validation of device types during P2P search in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Woice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking	qualcomm.co m/company/ product- security/bull etins/august-	
Exposure of Resource to Wrong Sphere08-Sep-212.1information from parent process due to numeric pids are getting compared and these pid can be reused in Snapdragon Auto, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile,https://www. qualcomm.co m/company/ product- security/bull etins/august- 2021-bulletinH-QUA-APQ8- 170921/419	apq8017					
	Resource to Wrong	08-Sep-21	2.1	information from parent process due to numeric pids are getting compared and these pid can be reused in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile,	qualcomm.co m/company/ product- security/bull etins/august-	

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Snapdragon Wearables		
			CVE ID : CVE-2021-1904		
Loop with Unreachable Exit Condition ('Infinite Loop')	08-Sep-21	5	Loop with unreachable exit condition may occur due to improper handling of unsupported input in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Voice & Music, Snapdragon Wearables CVE ID : CVE-2021-1914	https://www. qualcomm.co m/company/ product- security/bull etins/august- 2021-bulletin	H-QUA-APQ8- 170921/420
Out-of- bounds Write	08-Sep-21	10	Possible buffer underflow due to lack of check for negative indices values when processing user provided input in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Voice & Music, Snapdragon Wearables CVE ID : CVE-2021-1916	https://www. qualcomm.co m/company/ product- security/bull etins/august- 2021-bulletin	H-QUA-APQ8- 170921/421
Integer Underflow (Wrap or Wraparoun d)	08-Sep-21	10	Integer underflow can occur when the RTCP length is lesser than than the actual blocks present in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Voice & Music, Snapdragon	https://www. qualcomm.co m/company/ product- security/bull etins/august- 2021-bulletin	H-QUA-APQ8- 170921/422

0-1

1-2

5-6

6-7

7-8

8-9

		XA7]]						
		Wearables						
		CVE ID : CVE-2021-1919						
08-Sep-21	10	Integer underflow can occur due to improper handling of incoming RTCP packets in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Voice & Music, Snapdragon Wearables	https://www. qualcomm.co m/company/ product- security/bull etins/august- 2021-bulletin	H-QUA-APQ8- 170921/423				
		CVE ID : CVE-2021-1920						
08-Sep-21	10	Possible buffer overflow due to improper validation of device types during P2P search in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Woice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking CVE ID : CVE-2021-1972	https://www. qualcomm.co m/company/ product- security/bull etins/august- 2021-bulletin	H-QUA-APQ8- 170921/424				
apq8037								
08-Sep-21	5	Loop with unreachable exit condition may occur due to improper handling of unsupported input in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT,	https://www. qualcomm.co m/company/ product- security/bull etins/august- 2021-bulletin	H-QUA-APQ8- 170921/425				
	08-Sep-21	08-Sep-21 10 08-Sep-21 5	08-Sep-2110incoming RTCP packets in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Voice & Music, Snapdragon Wearables08-Sep-2110Possible buffer overflow due to improper validation of device types during P2P search in Snapdragon Auto, Snapdragon Consumer IOT, Snapdragon Compute, Snapdragon Compute, Snapdragon Consumer IOT, Snapdragon Consumer IOT, Snapdragon Consumer IOT, Snapdragon Consumer IOT, Snapdragon Nobile, Snapdragon Nobile, Snapdragon Wearables, Snapdragon Wied Infrastructure and Networking08-Sep-2110Loop with unreachable exit condition may occur due to improper handling of unsupported input in Snapdragon Compute, Snapdragon Auto, Snapdragon Auto, Snapdragon Wied Infrastructure and Networking08-Sep-215Loop with unreachable exit condition may occur due to improper handling of unsupported input in Snapdragon Connectivity, Snapdragon Consumer IOT,	08-Sep-2110incoming RTCP packets in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Industrial IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Voice & Music, Snapdragonhttps://www. qualcomm.co m/company/ product- security/bull etins/august- 2021-bulletin08-Sep-2110Possible buffer overflow due to improper validation of device types during P2P search in Snapdragon Auto, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Consumer IOT, Snapdragon Noice & Music, Snapdragon Wearables, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networkinghttps://www. qualcomm.co m/company/ product- security/bull etins/august- 2021-bulletin08-Sep-215Loop with unreachable exit condition may occur due to improper handling of unsupported input in Snapdragon Connectivity, Snapdragon Connectivity, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Consumer IOT, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networkinghttps://www. qualcomm.co m/company/ product- security/bull etins/august- 2021-bulletin08-Sep-215Loop with unreachable exit condition may occur due to improper handling of unsupported input in Snapdragon Connectivity, Snapdragon Connect				

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Voice & Music, Snapdragon Wearables CVE ID : CVE-2021-1914		
Out-of- bounds Write	08-Sep-21	10	Possible buffer underflow due to lack of check for negative indices values when processing user provided input in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Voice & Music, Snapdragon Wearables CVE ID : CVE-2021-1916	https://www. qualcomm.co m/company/ product- security/bull etins/august- 2021-bulletin	H-QUA-APQ8- 170921/426
Integer Underflow (Wrap or Wraparoun d)	08-Sep-21	10	Integer underflow can occur when the RTCP length is lesser than than the actual blocks present in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Voice & Music, Snapdragon Wearables CVE ID : CVE-2021-1919	https://www. qualcomm.co m/company/ product- security/bull etins/august- 2021-bulletin	H-QUA-APQ8- 170921/427
Integer Underflow (Wrap or Wraparoun d)	08-Sep-21	10	Integer underflow can occur due to improper handling of incoming RTCP packets in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT,	https://www. qualcomm.co m/company/ product- security/bull etins/august- 2021-bulletin	H-QUA-APQ8- 170921/428

1-2

0-1

6-7

5-6

7-8

8-9

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Snapdragon IoT, Snapdragon Voice & Music, Snapdragon Wearables		
			CVE ID : CVE-2021-1920		
apq8053					
Exposure of Resource to Wrong Sphere	08-Sep-21	2.1	Child process can leak information from parent process due to numeric pids are getting compared and these pid can be reused in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wearables CVE ID : CVE-2021-1904	https://www. qualcomm.co m/company/ product- security/bull etins/august- 2021-bulletin	H-QUA-APQ8- 170921/429
Loop with Unreachable Exit Condition ('Infinite Loop')	08-Sep-21	5	Loop with unreachable exit condition may occur due to improper handling of unsupported input in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Voice & Music, Snapdragon Wearables CVE ID : CVE-2021-1914	https://www. qualcomm.co m/company/ product- security/bull etins/august- 2021-bulletin	H-QUA-APQ8- 170921/430
Out-of- bounds Write	08-Sep-21	10	Possible buffer underflow due to lack of check for negative indices values when processing user provided input in Snapdragon Auto, Snapdragon Compute,	https://www. qualcomm.co m/company/ product- security/bull etins/august-	H-QUA-APQ8- 170921/431
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 & CVE ID	Patch	NCIIPC ID
			Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Voice & Music, Snapdragon Wearables	2021-bulletin	
			CVE ID : CVE-2021-1916		
Integer Underflow (Wrap or Wraparoun d)	08-Sep-21	10	Integer underflow can occur when the RTCP length is lesser than than the actual blocks present in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Voice & Music, Snapdragon Wearables	https://www. qualcomm.co m/company/ product- security/bull etins/august- 2021-bulletin	H-QUA-APQ8- 170921/432
			CVE ID : CVE-2021-1919		
Integer Underflow (Wrap or Wraparoun d)	08-Sep-21	10	Integer underflow can occur due to improper handling of incoming RTCP packets in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Voice & Music, Snapdragon Wearables CVE ID : CVE-2021-1920	https://www. qualcomm.co m/company/ product- security/bull etins/august- 2021-bulletin	H-QUA-APQ8- 170921/433
Out-of- bounds Read	08-Sep-21	3.6	Buffer over read could occur due to incorrect check of buffer size while flashing emmc devices in Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon	https://www. qualcomm.co m/company/ product- security/bull etins/august- 2021-bulletin	H-QUA-APQ8- 170921/434
CVSS Scoring Sca	ale 0-1	1-2	2-3 3-4 4-5 5-6	6-7 7-8	8-9 9-10

 3-4
 4-5
 5-6
 6-7

 Page 161 of 1474

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Mobile, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking CVE ID : CVE-2021-1928		
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	08-Sep-21	10	Possible buffer overflow due to improper validation of device types during P2P search in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Industrial IOT, Snapdragon Woice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking CVE ID : CVE-2021-1972	https://www. qualcomm.co m/company/ product- security/bull etins/august- 2021-bulletin	H-QUA-APQ8- 170921/435
apq8064au					
Exposure of Resource to Wrong Sphere	08-Sep-21	2.1	Child process can leak information from parent process due to numeric pids are getting compared and these pid can be reused in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wearables CVE ID : CVE-2021-1904	https://www. qualcomm.co m/company/ product- security/bull etins/august- 2021-bulletin	H-QUA-APQ8- 170921/436
Buffer Copy without	08-Sep-21	10	Possible buffer overflow due to improper validation of	https://www. qualcomm.co	H-QUA-APQ8- 170921/437

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Checking Size of Input ('Classic Buffer Overflow')			device types during P2P search in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Woice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking CVE ID : CVE-2021-1972	m/company/ product- security/bull etins/august- 2021-bulletin	
apq8076					
Exposure of Resource to Wrong Sphere	08-Sep-21	2.1	Child process can leak information from parent process due to numeric pids are getting compared and these pid can be reused in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables CVE ID : CVE-2021-1904	https://www. qualcomm.co m/company/ product- security/bull etins/august- 2021-bulletin	H-QUA-APQ8- 170921/438
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	08-Sep-21	10	Possible buffer overflow due to improper validation of device types during P2P search in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables,	https://www. qualcomm.co m/company/ product- security/bull etins/august- 2021-bulletin	H-QUA-APQ8- 170921/439

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Snapdragon Wired Infrastructure and Networking		
			CVE ID : CVE-2021-1972		
apq8084	ſ				
Out-of- bounds Write	08-Sep-21	10	Possible buffer underflow due to lack of check for negative indices values when processing user provided input in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Voice & Music, Snapdragon Wearables	https://www. qualcomm.co m/company/ product- security/bull etins/august- 2021-bulletin	H-QUA-APQ8- 170921/440
			CVE ID : CVE-2021-1916		
Integer Underflow (Wrap or Wraparoun d)	08-Sep-21	10	Integer underflow can occur when the RTCP length is lesser than than the actual blocks present in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Voice & Music, Snapdragon Wearables	https://www. qualcomm.co m/company/ product- security/bull etins/august- 2021-bulletin	H-QUA-APQ8- 170921/441
			CVE ID : CVE-2021-1919		
Integer Underflow (Wrap or Wraparoun d)	08-Sep-21	10	Integer underflow can occur due to improper handling of incoming RTCP packets in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT,	https://www. qualcomm.co m/company/ product- security/bull etins/august- 2021-bulletin	H-QUA-APQ8- 170921/442
CVSS Scoring Sc	ale 0-1	1-2	2-3 3-4 4-5 5-6 Page 164 of 1474	6-7 7-8	8-9 9-10

Page 164 of 1474

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Snapdragon IoT, Snapdragon Voice & Music, Snapdragon Wearables		
			CVE ID : CVE-2021-1920		
apq8096au					
Exposure of Resource to Wrong Sphere	08-Sep-21	2.1	Child process can leak information from parent process due to numeric pids are getting compared and these pid can be reused in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wearables CVE ID : CVE-2021-1904	https://www. qualcomm.co m/company/ product- security/bull etins/august- 2021-bulletin	H-QUA-APQ8- 170921/443
Loop with Unreachable Exit Condition ('Infinite Loop')	08-Sep-21	5	Loop with unreachable exit condition may occur due to improper handling of unsupported input in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Voice & Music, Snapdragon Wearables CVE ID : CVE-2021-1914	https://www. qualcomm.co m/company/ product- security/bull etins/august- 2021-bulletin	H-QUA-APQ8- 170921/444
Out-of- bounds Write	08-Sep-21	10	Possible buffer underflow due to lack of check for negative indices values when processing user provided input in Snapdragon Auto, Snapdragon Compute,	https://www. qualcomm.co m/company/ product- security/bull etins/august-	H-QUA-APQ8- 170921/445
CVSS Scoring Sc	ale 0-1	1-2	2-3 3-4 4-5 5-6	6-7 7-8	8-9 9-10

				NCIIPC ID
		Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Voice & Music, Snapdragon Wearables	2021-bulletin	
		CVE ID : CVE-2021-1916		
08-Sep-21	10	Integer underflow can occur when the RTCP length is lesser than than the actual blocks present in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Voice & Music, Snapdragon Wearables	https://www. qualcomm.co m/company/ product- security/bull etins/august- 2021-bulletin	H-QUA-APQ8- 170921/446
		CVE ID : CVE-2021-1919		
08-Sep-21	10	Integer underflow can occur due to improper handling of incoming RTCP packets in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Voice & Music, Snapdragon Wearables CVE ID : CVE-2021-1920	https://www. qualcomm.co m/company/ product- security/bull etins/august- 2021-bulletin	H-QUA-APQ8- 170921/447
08-Sep-21	2.1	Lack of strict validation of bootmode can lead to information disclosure in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT,	https://www. qualcomm.co m/company/ product- security/bull etins/august- 2021-bulletin	H-QUA-APQ8- 170921/448
	08-Sep-21	08-Sep-21 10 08-Sep-21 2.1	08-Sep-21Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Voice & Music, Snapdragon Wearables08-Sep-21Integer underflow can occur when the RTCP length is lesser than than the actual blocks present in Snapdragon Auto, Snapdragon Compute, Snapdragon Industrial IOT, Snapdragon Auto, Snapdragon Compute, Snapdragon Compute, Snapdragon Industrial IOT, Snapdragon Industrial IOT, Snapdrag	Image: state in the state interval to the state int

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wearables		
			CVE ID : CVE-2021-1929		
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	08-Sep-21	10	Possible buffer overflow due to improper validation of device types during P2P search in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Woice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking CVE ID : CVE-2021-1972	https://www. qualcomm.co m/company/ product- security/bull etins/august- 2021-bulletin	H-QUA-APQ8- 170921/449
aqt1000					
Exposure of Resource to Wrong Sphere	08-Sep-21	2.1	Child process can leak information from parent process due to numeric pids are getting compared and these pid can be reused in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wearables CVE ID : CVE-2021-1904	https://www. qualcomm.co m/company/ product- security/bull etins/august- 2021-bulletin	H-QUA-AQT1- 170921/450
Loop with Unreachable Exit Condition	08-Sep-21	5	Loop with unreachable exit condition may occur due to improper handling of unsupported input in	https://www. qualcomm.co m/company/ product-	H-QUA-AQT1- 170921/451
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 & CVE ID	Patch	NCIIPC ID
('Infinite Loop')			Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Voice & Music, Snapdragon Wearables CVE ID : CVE-2021-1914	security/bull etins/august- 2021-bulletin	
Out-of- bounds Write	08-Sep-21	10	Possible buffer underflow due to lack of check for negative indices values when processing user provided input in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Voice & Music, Snapdragon Wearables CVE ID : CVE-2021-1916	https://www. qualcomm.co m/company/ product- security/bull etins/august- 2021-bulletin	H-QUA-AQT1- 170921/452
Integer Underflow (Wrap or Wraparoun d)	08-Sep-21	10	Integer underflow can occur when the RTCP length is lesser than than the actual blocks present in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Voice & Music, Snapdragon Wearables CVE ID : CVE-2021-1919	https://www. qualcomm.co m/company/ product- security/bull etins/august- 2021-bulletin	H-QUA-AQT1- 170921/453
Integer Underflow (Wrap or Wraparoun	08-Sep-21	10	Integer underflow can occur due to improper handling of incoming RTCP packets in Snapdragon Auto,	https://www. qualcomm.co m/company/ product-	H-QUA-AQT1- 170921/454

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

Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
		Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Voice & Music, Snapdragon Wearables CVE ID : CVE-2021-1920	security/bull etins/august- 2021-bulletin	
08-Sep-21	4.6	Incorrect pointer argument passed to trusted application TA could result in un- intended memory operations in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Industrial IOT CVE ID : CVE-2021-1923	https://www. qualcomm.co m/company/ product- security/bull etins/august- 2021-bulletin	H-QUA-AQT1- 170921/455
08-Sep-21	2.1	Lack of strict validation of bootmode can lead to information disclosure in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wearables CVE ID : CVE-2021-1929	https://www. qualcomm.co m/company/ product- security/bull etins/august- 2021-bulletin	H-QUA-AQT1- 170921/456
08-Sep-21	3.6	Possible out of bounds read due to incorrect validation of incoming buffer length in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile CVE ID : CVE-2021-1930	https://www. qualcomm.co m/company/ product- security/bull etins/august- 2021-bulletin	H-QUA-AQT1- 170921/457
	08-Sep-21	08-Sep-21 4.6 08-Sep-21 2.1	Image: construct of the structure of the	Image: constraint of the standard of the stand

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	08-Sep-21	10	Possible buffer overflow due to improper validation of device types during P2P search in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Woice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking CVE ID : CVE-2021-1972	https://www. qualcomm.co m/company/ product- security/bull etins/august- 2021-bulletin	H-QUA-AQT1- 170921/458
ar6003					
Out-of- bounds Write	08-Sep-21	10	Possible buffer underflow due to lack of check for negative indices values when processing user provided input in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Voice & Music, Snapdragon Wearables CVE ID : CVE-2021-1916	https://www. qualcomm.co m/company/ product- security/bull etins/august- 2021-bulletin	H-QUA-AR60- 170921/459
Integer Underflow (Wrap or Wraparoun d)	08-Sep-21	10	Integer underflow can occur due to improper handling of incoming RTCP packets in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Voice & Music, Snapdragon	https://www. qualcomm.co m/company/ product- security/bull etins/august- 2021-bulletin	H-QUA-AR60- 170921/460

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID				
			Wearables						
			CVE ID : CVE-2021-1920						
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	08-Sep-21	10	Possible buffer overflow due to improper validation of device types during P2P search in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Woice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking CVE ID : CVE-2021-1972	https://www. qualcomm.co m/company/ product- security/bull etins/august- 2021-bulletin	H-QUA-AR60- 170921/461				
ar7420									
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	08-Sep-21	10	Possible buffer overflow due to improper validation of device types during P2P search in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Industrial IOT, Snapdragon Woile, Snapdragon Woice & Music, Snapdragon Wired Infrastructure and Networking CVE ID : CVE-2021-1972	https://www. qualcomm.co m/company/ product- security/bull etins/august- 2021-bulletin	H-QUA-AR74- 170921/462				
ar8031					<u> </u>				
Exposure of Resource to Wrong	08-Sep-21	2.1	Child process can leak information from parent process due to numeric pids are getting compared and	https://www. qualcomm.co m/company/ product-	H-QUA-AR80- 170921/463				
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 & CVE ID	Patch	NCIIPC ID
Sphere			these pid can be reused in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables CVE ID : CVE-2021-1904	security/bull etins/august- 2021-bulletin	
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	08-Sep-21	10	Possible buffer overflow due to improper validation of device types during P2P search in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Industrial IOT, Snapdragon Woile, Snapdragon Woice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking CVE ID : CVE-2021-1972	https://www. qualcomm.co m/company/ product- security/bull etins/august- 2021-bulletin	H-QUA-AR80- 170921/464
ar8035				I	
Exposure of Resource to Wrong Sphere	08-Sep-21	2.1	Child process can leak information from parent process due to numeric pids are getting compared and these pid can be reused in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music,	https://www. qualcomm.co m/company/ product- security/bull etins/august- 2021-bulletin	H-QUA-AR80- 170921/465

CVSS Scoring Scale	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10
			Pa	age 172 c	of 1474					

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID								
			Snapdragon Wearables										
			CVE ID : CVE-2021-1904										
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	08-Sep-21	10	Possible buffer overflow due to improper validation of device types during P2P search in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Woice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking	https://www. qualcomm.co m/company/ product- security/bull etins/august- 2021-bulletin	H-QUA-AR80- 170921/466								
CVE ID : CVE-2021-1972													
Out-of- bounds Read	08-Sep-21	3.6	Buffer over read could occur due to incorrect check of buffer size while flashing emmc devices in Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking CVE ID : CVE-2021-1928	https://www. qualcomm.co m/company/ product- security/bull etins/august- 2021-bulletin	H-QUA-AR93- 170921/467								
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	08-Sep-21	10	Possible buffer overflow due to improper validation of device types during P2P search in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT,	https://www. qualcomm.co m/company/ product- security/bull etins/august- 2021-bulletin	H-QUA-AR93- 170921/468								
CVSS Scoring Sca	ale 0-1	1-2	2-3 3-4 4-5 5-6 Page 173 of 1474	6-7 7-8									

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking		
csr6030			CVE ID : CVE-2021-1972		
Exposure of Resource to Wrong Sphere	08-Sep-21	2.1	Child process can leak information from parent process due to numeric pids are getting compared and these pid can be reused in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wearables CVE ID : CVE-2021-1904	https://www. qualcomm.co m/company/ product- security/bull etins/august- 2021-bulletin	H-QUA-CSR6- 170921/469
Loop with Unreachable Exit Condition ('Infinite Loop')	08-Sep-21	5	Loop with unreachable exit condition may occur due to improper handling of unsupported input in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Voice & Music, Snapdragon Wearables CVE ID : CVE-2021-1914	https://www. qualcomm.co m/company/ product- security/bull etins/august- 2021-bulletin	H-QUA-CSR6- 170921/470
Out-of- bounds	08-Sep-21	10	Possible buffer underflow due to lack of check for	https://www. qualcomm.co	H-QUA-CSR6- 170921/471

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Write			negative indices values when processing user provided input in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Voice & Music, Snapdragon Wearables CVE ID : CVE-2021-1916	m/company/ product- security/bull etins/august- 2021-bulletin	
Integer Underflow (Wrap or Wraparoun d)	08-Sep-21	10	Integer underflow can occur when the RTCP length is lesser than than the actual blocks present in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Voice & Music, Snapdragon Wearables CVE ID : CVE-2021-1919	https://www. qualcomm.co m/company/ product- security/bull etins/august- 2021-bulletin	H-QUA-CSR6- 170921/472
Integer Underflow (Wrap or Wraparoun d)	08-Sep-21	10	Integer underflow can occur due to improper handling of incoming RTCP packets in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Voice & Music, Snapdragon Wearables	https://www. qualcomm.co m/company/ product- security/bull etins/august- 2021-bulletin	H-QUA-CSR6- 170921/473
Buffer Copy			CVE ID : CVE-2021-1920 Possible buffer overflow due	https://www.	H-QUA-CSR6-
without Checking	08-Sep-21	10	to improper validation of device types during P2P	qualcomm.co m/company/	170921/474

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

Page 176 of 1474

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID						
			Networking								
			CVE ID : CVE-2021-1972								
csra6620											
Exposure of Resource to Wrong Sphere	08-Sep-21	2.1	Child process can leak information from parent process due to numeric pids are getting compared and these pid can be reused in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wearables CVE ID : CVE-2021-1904	https://www. qualcomm.co m/company/ product- security/bull etins/august- 2021-bulletin	H-QUA-CSRA- 170921/477						
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	08-Sep-21	10	Possible buffer overflow due to improper validation of device types during P2P search in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Industrial IOT, Snapdragon Woile, Snapdragon Woice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking CVE ID : CVE-2021-1972	https://www. qualcomm.co m/company/ product- security/bull etins/august- 2021-bulletin	H-QUA-CSRA- 170921/478						
csra6640											
Exposure of Resource to Wrong Sphere	08-Sep-21	2.1	Child process can leak information from parent process due to numeric pids are getting compared and these pid can be reused in	https://www. qualcomm.co m/company/ product- security/bull	H-QUA-CSRA- 170921/479						
CVSS Scoring Sc	ale 0-1	1-2	2-3 3-4 4-5 5-6 Page 177 of 1474	6-7 7-8	CVSS Scoring Scale 0-1 1-2 2-3 3-4 4-5 5-6 6-7 7-8 8-9 9-10						

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables CVE ID : CVE-2021-1904	etins/august- 2021-bulletin	
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	08-Sep-21	10	Possible buffer overflow due to improper validation of device types during P2P search in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Woice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking CVE ID : CVE-2021-1972	https://www. qualcomm.co m/company/ product- security/bull etins/august- 2021-bulletin	H-QUA-CSRA- 170921/480
csrb31024					
Exposure of Resource to Wrong Sphere	osure of ource to ng ere 08-Sep-21 2.1 Snap Snap Snap Snap Snap Snap Snap Snap		Child process can leak information from parent process due to numeric pids are getting compared and these pid can be reused in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables	https://www. qualcomm.co m/company/ product- security/bull etins/august- 2021-bulletin	H-QUA-CSRB- 170921/481

CVSS Scoring Scale	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10
			Р	age 178 c	of 1474					

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2021-1904		
Loop with Unreachable Exit Condition ('Infinite Loop')	08-Sep-21	5	Loop with unreachable exit condition may occur due to improper handling of unsupported input in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Voice & Music, Snapdragon Wearables CVE ID : CVE-2021-1914	https://www. qualcomm.co m/company/ product- security/bull etins/august- 2021-bulletin	H-QUA-CSRB- 170921/482
Out-of- bounds Write	08-Sep-21	10	Possible buffer underflow due to lack of check for negative indices values when processing user provided input in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Voice & Music, Snapdragon Wearables CVE ID : CVE-2021-1916	https://www. qualcomm.co m/company/ product- security/bull etins/august- 2021-bulletin	H-QUA-CSRB- 170921/483
Integer Underflow (Wrap or Wraparoun d)	08-Sep-21	10	Integer underflow can occur when the RTCP length is lesser than than the actual blocks present in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Voice & Music, Snapdragon Wearables	https://www. qualcomm.co m/company/ product- security/bull etins/august- 2021-bulletin	H-QUA-CSRB- 170921/484

0-1

1-2

4-5

5-6

6-7

7-8

8-9

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2021-1919		
Integer Underflow (Wrap or Wraparoun d)	08-Sep-21	10	Integer underflow can occur due to improper handling of incoming RTCP packets in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Voice & Music, Snapdragon Wearables CVE ID : CVE-2021-1920	https://www. qualcomm.co m/company/ product- security/bull etins/august- 2021-bulletin	H-QUA-CSRB- 170921/485
Improper Restriction of Operations within the Bounds of a Memory Buffer	08-Sep-21	3.6	Possible out of bounds read due to incorrect validation of incoming buffer length in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile CVE ID : CVE-2021-1930	https://www. qualcomm.co m/company/ product- security/bull etins/august- 2021-bulletin	H-QUA-CSRB- 170921/486
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	08-Sep-21	10	Possible buffer overflow due to improper validation of device types during P2P search in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Woice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking CVE ID : CVE-2021-1972	https://www. qualcomm.co m/company/ product- security/bull etins/august- 2021-bulletin	H-QUA-CSRB- 170921/487

 3-4
 4-5
 5-6

 Page 180 of 1474

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID			
fsm10055	fsm10055							
Exposure of Resource to Wrong Sphere	08-Sep-21	2.1	Child process can leak information from parent process due to numeric pids are getting compared and these pid can be reused in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wearables CVE ID : CVE-2021-1904	https://www. qualcomm.co m/company/ product- security/bull etins/august- 2021-bulletin	H-QUA-FSM1- 170921/488			
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	08-Sep-21	10	Possible buffer overflow due to improper validation of device types during P2P search in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Woice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking CVE ID : CVE-2021-1972	https://www. qualcomm.co m/company/ product- security/bull etins/august- 2021-bulletin	H-QUA-FSM1- 170921/489			
fsm10056				<u> </u>				
Exposure of Resource to Wrong Sphere	08-Sep-21	2.1	Child process can leak information from parent process due to numeric pids are getting compared and these pid can be reused in Snapdragon Auto, Snapdragon Compute,	https://www. qualcomm.co m/company/ product- security/bull etins/august- 2021-bulletin	H-QUA-FSM1- 170921/490			
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 & CVE ID	Patch	NCIIPC ID
			Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables		
			CVE ID : CVE-2021-1904		
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	08-Sep-21	10	Possible buffer overflow due to improper validation of device types during P2P search in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Woice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking CVE ID : CVE-2021-1972	https://www. qualcomm.co m/company/ product- security/bull etins/august- 2021-bulletin	H-QUA-FSM1- 170921/491
ipq4018					
Out-of- bounds Read	08-Sep-21	3.6	Buffer over read could occur due to incorrect check of buffer size while flashing emmc devices in Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking CVE ID : CVE-2021-1928	https://www. qualcomm.co m/company/ product- security/bull etins/august- 2021-bulletin	H-QUA-IPQ4- 170921/492
Buffer Copy without	08-Sep-21	10	Possible buffer overflow due to improper validation of	https://www. qualcomm.co	H-QUA-IPQ4- 170921/493

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Checking Size of Input ('Classic Buffer Overflow')			device types during P2P search in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Woice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking CVE ID : CVE-2021-1972	m/company/ product- security/bull etins/august- 2021-bulletin	
ipq4019					
Out-of- bounds Read	08-Sep-21	3.6	Buffer over read could occur due to incorrect check of buffer size while flashing emmc devices in Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking CVE ID : CVE-2021-1928	https://www. qualcomm.co m/company/ product- security/bull etins/august- 2021-bulletin	H-QUA-IPQ4- 170921/494
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	08-Sep-21	10	Possible buffer overflow due to improper validation of device types during P2P search in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wired	https://www. qualcomm.co m/company/ product- security/bull etins/august- 2021-bulletin	H-QUA-IPQ4- 170921/495

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Infrastructure and Networking		
			C		
			CVE ID : CVE-2021-1972		
ipq4028					
Out-of- bounds Read	08-Sep-21	3.6	Buffer over read could occur due to incorrect check of buffer size while flashing emmc devices in Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking CVE ID : CVE-2021-1928	https://www. qualcomm.co m/company/ product- security/bull etins/august- 2021-bulletin	H-QUA-IPQ4- 170921/496
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	08-Sep-21	10	Possible buffer overflow due to improper validation of device types during P2P search in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Woice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking CVE ID : CVE-2021-1972	https://www. qualcomm.co m/company/ product- security/bull etins/august- 2021-bulletin	H-QUA-IPQ4- 170921/497
ipq4029					
Out-of- bounds Read	08-Sep-21	3.6	Buffer over read could occur due to incorrect check of buffer size while flashing emmc devices in Snapdragon Connectivity, Snapdragon	https://www. qualcomm.co m/company/ product- security/bull	H-QUA-IPQ4- 170921/498
		3.6	buffer size while flashing emmc devices in Snapdragon	m/compan product- security/b	ny/

Page 184 of 1474

Buffer Copy without Checking Size of Input (Classic Buffer Copy' without Checking Size of Input (Classic Buffer Direction)Image Compute Search in Snapdragon Mobile, Snapdragon Core & Wearables, Snapdragon Wearables, Snapdragon Wearables, Snapdragon Auto, Snapdragon Consumer 107, Snapdragon Mobile, Snapdragon Ouse Mobile, Snapdragon Ouse Mobile, Snapdragon Ouse Mobile, Snapdragon Consumer 107, Snapdragon Mobile, Snapdragon Ouse Mobile, Snapdragon Ouse Mobile, Snapdragon Ouse Mobile, Snapdragon Mobile, Snapdragon Mobile, Snapdragon Ouse Mobile, Snapdragon Mobile, Snapdragon Mobile, Snapdragon Mobile, Snapdragon Mobile, Snapdragon Wired Infrastructure and Networking COVE DI : CVE-2021-1922Https://www. H-QUA-IPQ4- 170921/499Out-of- bounds Read08-Sep-218.Buffer Over read could occur due to incorrect check of buffer size while flashing emmc devices in Snapdragon Consentivity, Snapdragon Mobile, Snapdragon Consentivity, Snapdragon Mobile, Snapdragon Mobile, Snapdragon Mobile, Snapdragon Security/bull etins/august- 2021-bulletinH-QUA-IPQ5- 170921/500Out-of- bounds Read08-Sep-218.MBuffer Overflow due ter Vervorking COnsumer 107, Snapdragon Mobile, Snapdragon Consumer 107, Snapdragon Mobile, Snapdragon Mobile, Snapdragon Mobile, Snapdragon Mobile, Snapdragon Mobile, Snapdragon Mobile, Snapdragon Mobile, Snapdragon Mobile, Snapdragon Mobile, Snapdragon Mobi	Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')Image: Subscript of the security of the				Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking		
Out-of- bounds Read08-Sep-218.6 a.6Buffer over read could occur due to incorrect check of buffer size while flashing emmc devices in Snapdragon Connectivity, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Mobile, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networkinghttps://www. qualcomm.co m/company/ 	without Checking Size of Input ('Classic Buffer	08-Sep-21	10	to improper validation of device types during P2P search in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Woice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking	qualcomm.co m/company/ product- security/bull etins/august-	
Out-of- bounds Read08-Sep-213.6due to incorrect check of buffer size while flashing emmc devices in Snapdragon Connectivity, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networkinghttps://www. qualcomm.co m/company/ product- security/bull etins/august- 2021-bulletinH-QUA-IPQ5- 170921/500	ipq5010					
Buffer Copy 08-Sep-21 10 Possible buffer overflow due https://www. H-QUA-IPQ5-	bounds	08-Sep-21	3.6	due to incorrect check of buffer size while flashing emmc devices in Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking	qualcomm.co m/company/ product- security/bull etins/august-	
	Buffer Copy	08-Sep-21	10	Possible buffer overflow due	https://www.	H-QUA-IPQ5-

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
without Checking Size of Input ('Classic Buffer Overflow')			to improper validation of device types during P2P search in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Woice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking	qualcomm.co m/company/ product- security/bull etins/august- 2021-bulletin	170921/501
in = 5 010			CVE ID : CVE-2021-1972		
ipq5018					
Out-of- bounds Read	08-Sep-21	3.6	Buffer over read could occur due to incorrect check of buffer size while flashing emmc devices in Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking CVE ID : CVE-2021-1928	https://www. qualcomm.co m/company/ product- security/bull etins/august- 2021-bulletin	H-QUA-IPQ5- 170921/502
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	08-Sep-21	10	Possible buffer overflow due to improper validation of device types during P2P search in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables,	https://www. qualcomm.co m/company/ product- security/bull etins/august- 2021-bulletin	H-QUA-IPQ5- 170921/503

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Snapdragon Wired Infrastructure and Networking CVE ID : CVE-2021-1972		
ipq5028					
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	08-Sep-21	10	Possible buffer overflow due to improper validation of device types during P2P search in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Woice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking CVE ID : CVE-2021-1972	https://www. qualcomm.co m/company/ product- security/bull etins/august- 2021-bulletin	H-QUA-IPQ5- 170921/504
ipq6000					
Out-of- bounds Read	08-Sep-21	3.6	Buffer over read could occur due to incorrect check of buffer size while flashing emmc devices in Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking CVE ID : CVE-2021-1928	https://www. qualcomm.co m/company/ product- security/bull etins/august- 2021-bulletin	H-QUA-IPQ6- 170921/505
Buffer Copy without Checking Size of Input CVSS Scoring Sc	08-Sep-21	10	Possible buffer overflow due to improper validation of device types during P2P search in Snapdragon Auto,	https://www. qualcomm.co m/company/ product-	H-QUA-IPQ6- 170921/506 8-9 9-10

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
('Classic Buffer Overflow')			Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking CVE ID : CVE-2021-1972	security/bull etins/august- 2021-bulletin	
ipq6005					
Out-of- bounds Read	08-Sep-21	3.6	Buffer over read could occur due to incorrect check of buffer size while flashing emmc devices in Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking CVE ID : CVE-2021-1928	https://www. qualcomm.co m/company/ product- security/bull etins/august- 2021-bulletin	H-QUA-IPQ6- 170921/507
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	08-Sep-21	10	Possible buffer overflow due to improper validation of device types during P2P search in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Woice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and	https://www. qualcomm.co m/company/ product- security/bull etins/august- 2021-bulletin	H-QUA-IPQ6- 170921/508

CVSS Scoring Scale	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10
			Pa	age 188 c	of 1474					

Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
		Networking		
		CVE ID : CVE-2021-1972		
08-Sep-21	3.6	Buffer over read could occur due to incorrect check of buffer size while flashing emmc devices in Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking CVE ID : CVE-2021-1928	https://www. qualcomm.co m/company/ product- security/bull etins/august- 2021-bulletin	H-QUA-IPQ6- 170921/509
08-Sep-21	10	Possible buffer overflow due to improper validation of device types during P2P search in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Woice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking	https://www. qualcomm.co m/company/ product- security/bull etins/august- 2021-bulletin	H-QUA-IPQ6- 170921/510
08-Sep-21	3.6	Buffer over read could occur due to incorrect check of buffer size while flashing emmc devices in Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon	https://www. qualcomm.co m/company/ product- security/bull etins/august-	H-QUA-IPQ6- 170921/511
	08-Sep-21	08-Sep-21 3.6 08-Sep-21 10	Image: Normal state in the s	NetworkingImage: CVE ID : CVE-2021-1972CVE ID : CVE-2021-1972CVE ID : CVE-2021-1972CVE ID : CVE-2021-1972Second Second

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking	2021-bulletin	
			CVE ID : CVE-2021-1928		
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	08-Sep-21	10	Possible buffer overflow due to improper validation of device types during P2P search in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Woice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking CVE ID : CVE-2021-1972	https://www. qualcomm.co m/company/ product- security/bull etins/august- 2021-bulletin	H-QUA-IPQ6- 170921/512
ipq6028					
Out-of- bounds Read	08-Sep-21	3.6	Buffer over read could occur due to incorrect check of buffer size while flashing emmc devices in Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking CVE ID : CVE-2021-1928	https://www. qualcomm.co m/company/ product- security/bull etins/august- 2021-bulletin	H-QUA-IPQ6- 170921/513
Buffer Copy without	08-Sep-21	10	Possible buffer overflow due to improper validation of	https://www. qualcomm.co	H-QUA-IPQ6- 170921/514

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Checking Size of Input ('Classic Buffer Overflow')			device types during P2P search in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Woice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking CVE ID : CVE-2021-1972	m/company/ product- security/bull etins/august- 2021-bulletin	
ipq8064					
Out-of- bounds Read	08-Sep-21	3.6	Buffer over read could occur due to incorrect check of buffer size while flashing emmc devices in Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking	https://www. qualcomm.co m/company/ product- security/bull etins/august- 2021-bulletin	H-QUA-IPQ8- 170921/515
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	08-Sep-21	10	CVE ID : CVE-2021-1928 Possible buffer overflow due to improper validation of device types during P2P search in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wearables, Snapdragon Wired	https://www. qualcomm.co m/company/ product- security/bull etins/august- 2021-bulletin	H-QUA-IPQ8- 170921/516

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID		
			Infrastructure and Networking				
			5				
			CVE ID : CVE-2021-1972				
ipq8065							
Out-of- bounds Read	08-Sep-21	3.6	Buffer over read could occur due to incorrect check of buffer size while flashing emmc devices in Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking CVE ID : CVE-2021-1928	https://www. qualcomm.co m/company/ product- security/bull etins/august- 2021-bulletin	H-QUA-IPQ8- 170921/517		
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	08-Sep-21	10	Possible buffer overflow due to improper validation of device types during P2P search in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Woice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking CVE ID : CVE-2021-1972	https://www. qualcomm.co m/company/ product- security/bull etins/august- 2021-bulletin	H-QUA-IPQ8- 170921/518		
ipq8068	ipq8068						
Out-of- bounds Read	08-Sep-21	3.6	Buffer over read could occur due to incorrect check of buffer size while flashing emmc devices in Snapdragon Connectivity, Snapdragon	https://www. qualcomm.co m/company/ product- security/bull	H-QUA-IPQ8- 170921/519		
CVSS Scoring Sc	ale 0-1	1-2	2-3 3-4 4-5 5-6 Page 192 of 1474	6-7 7-8	8-9 9-10		

Page 192 of 1474

Buffer Copy without Checking Size of Input (Classic Buffer Overflow')etins/august- august- 2021-bulletinetins/august- 2021-bulletin08-Sep-21 buffer Overflow')08-Sep-21 august- 2021-bulletinusic Snapdragon Moise Vired Infrastructure and Networking CVE D : CVE-2021-1928https://www. qualcomm.co m/company/ product- search in Snapdragon Mobile, Snapdragon Consumer 107, Snapdragon Consumer 107, Snapdragon Consumer 107, Snapdragon Mobile, Snapdragon Ouse & Music, Snapdragon Ouse & Music, Snapdragon Mobile, Snapdragon Mobile, Snapdragon Vice & Music, Snapdragon Vice & Music, Snapdragon Vice & Music, Snapdragon Vice & Music, Snapdragon Wierables, Snapdragon Mobile, Buffer Over read could occur due to incorrect check of buffer size while flashing emmc devices in Snapdragon Mobile, Snapdragon Music, Snapdragon Music, Snapdragon Wiera Infrastructure and Networking Comectivity, Snapdragon Wiera Infrastructure and Networking COP 10021-bulletinhttps://www. H-QUA-IPQ8- In0921/521 etins/august- 2021-bulletinBuffer	Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')Image: Stand and the st				Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking		
Out-of- bounds Read08-Sep-21B. Buffer over read could occur due to incorrect check of buffer size while flashing emmc devices in Snapdragon Connectivity, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Mosile, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networkinghttps://www. qualcomm.co m/company/ 	without Checking Size of Input ('Classic Buffer	08-Sep-21	10	to improper validation of device types during P2P search in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Woice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking	qualcomm.co m/company/ product- security/bull etins/august-	
Out-of- bounds Read08-Sep-213.6due to incorrect check of buffer size while flashing emmc devices in Snapdragon Connectivity, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networkinghttps://www. qualcomm.co m/company/ product- security/bull etins/august- 2021-bulletinH-QUA-IPQ8- 170921/521	ipq8069					
Buffer Copy 08-Sep-21 10 Possible buffer overflow due https://www. H-QUA-IPQ8-	bounds	08-Sep-21	3.6	due to incorrect check of buffer size while flashing emmc devices in Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking	qualcomm.co m/company/ product- security/bull etins/august-	
	Buffer Copy	08-Sep-21	10	Possible buffer overflow due	https://www.	H-QUA-IPQ8-

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID	
without Checking Size of Input ('Classic Buffer Overflow')			nput search in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity,		qualcomm.co m/company/ product- security/bull etins/august- 2021-bulletin	170921/522
in a 9070			CVE ID : CVE-2021-1972			
ipq8070			Duffen eren need er liter			
Out-of- bounds Read	08-Sep-21	3.6	Buffer over read could occur due to incorrect check of buffer size while flashing emmc devices in Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking CVE ID : CVE-2021-1928	https://www. qualcomm.co m/company/ product- security/bull etins/august- 2021-bulletin	H-QUA-IPQ8- 170921/523	
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow') CVSS Scoring Scale 0-1 1-2		Possible buffer overflow due to improper validation of device types during P2P search in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables,	https://www. qualcomm.co m/company/ product- security/bull etins/august- 2021-bulletin	H-QUA-IPQ8- 170921/524		

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID	
			Snapdragon Wired Infrastructure and Networking			
			CVE ID : CVE-2021-1972			
ipq8070a						
Out-of- bounds Read	08-Sep-21	3.6	Buffer over read could occur due to incorrect check of buffer size while flashing emmc devices in Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking	https://www. qualcomm.co m/company/ product- security/bull etins/august- 2021-bulletin	H-QUA-IPQ8- 170921/525	
			CVE ID : CVE-2021-1928			
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	08-Sep-21	10	Possible buffer overflow due to improper validation of device types during P2P search in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Woice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking CVE ID : CVE-2021-1972	https://www. qualcomm.co m/company/ product- security/bull etins/august- 2021-bulletin	H-QUA-IPQ8- 170921/526	
ipq8071						
Out-of- bounds Read	08-Sep-21	3.6	Buffer over read could occur due to incorrect check of buffer size while flashing emmc devices in Snapdragon	https://www. qualcomm.co m/company/ product-	H-QUA-IPQ8- 170921/527	
CVSS Scoring Sc	ale 0-1	1-2	2-3 3-4 4-5 5-6 Page 195 of 1474	6-7 7-8	8-9 9-10	

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking CVE ID : CVE-2021-1928	security/bull etins/august- 2021-bulletin	
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	08-Sep-21	10	Possible buffer overflow due to improper validation of device types during P2P search in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Industrial IOT, Snapdragon Woice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking CVE ID : CVE-2021-1972	https://www. qualcomm.co m/company/ product- security/bull etins/august- 2021-bulletin	H-QUA-IPQ8- 170921/528
ipq8071a	L			I	I
Out-of- bounds 08-Sep-21 3.6 Read			Buffer over read could occur due to incorrect check of buffer size while flashing emmc devices in Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking CVE ID : CVE-2021-1928	https://www. qualcomm.co m/company/ product- security/bull etins/august- 2021-bulletin	H-QUA-IPQ8- 170921/529
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 & CVE ID	Patch	NCIIPC ID
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	08-Sep-21	10	Possible buffer overflow due to improper validation of device types during P2P search in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Woice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking CVE ID : CVE-2021-1972	https://www. qualcomm.co m/company/ product- security/bull etins/august- 2021-bulletin	H-QUA-IPQ8- 170921/530
ipq8072					
Out-of- bounds Read	08-Sep-21	3.6	Buffer over read could occur due to incorrect check of buffer size while flashing emmc devices in Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking CVE ID : CVE-2021-1928	https://www. qualcomm.co m/company/ product- security/bull etins/august- 2021-bulletin	H-QUA-IPQ8- 170921/531
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	08-Sep-21	10	Possible buffer overflow due to improper validation of device types during P2P search in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music,	https://www. qualcomm.co m/company/ product- security/bull etins/august- 2021-bulletin	H-QUA-IPQ8- 170921/532

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking		
			CVE ID : CVE-2021-1972		
ipq8072a	L			I	L
Out-of- bounds Read	08-Sep-21	3.6	Buffer over read could occur due to incorrect check of buffer size while flashing emmc devices in Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking CVE ID : CVE-2021-1928	https://www. qualcomm.co m/company/ product- security/bull etins/august- 2021-bulletin	H-QUA-IPQ8- 170921/533
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	08-Sep-21	10	Possible buffer overflow due to improper validation of device types during P2P search in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Woice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking CVE ID : CVE-2021-1972	https://www. qualcomm.co m/company/ product- security/bull etins/august- 2021-bulletin	H-QUA-IPQ8- 170921/534
ipq8074					
Out-of- bounds	08-Sep-21	3.6	Buffer over read could occur due to incorrect check of buffer size while flashing	https://www. qualcomm.co m/company/	H-QUA-IPQ8- 170921/535
CVSS Scoring Sc	ale 0-1	1-2	2-3 3-4 4-5 5-6 Page 198 of 1474	6-7 7-8	8-9 9-10

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Read			emmc devices in Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking CVE ID : CVE-2021-1928	product- security/bull etins/august- 2021-bulletin	
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	08-Sep-21	10	Possible buffer overflow due to improper validation of device types during P2P search in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Industrial IOT, Snapdragon Woice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking CVE ID : CVE-2021-1972	https://www. qualcomm.co m/company/ product- security/bull etins/august- 2021-bulletin	H-QUA-IPQ8- 170921/536
ipq8074a					
Out-of- bounds Read	08-Sep-21	3.6	Buffer over read could occur due to incorrect check of buffer size while flashing emmc devices in Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking	https://www. qualcomm.co m/company/ product- security/bull etins/august- 2021-bulletin	H-QUA-IPQ8- 170921/537

CVSS Scoring Scale	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10
Page 199 of 1474										

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2021-1928		
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	08-Sep-21	10	Possible buffer overflow due to improper validation of device types during P2P search in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Woice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking	https://www. qualcomm.co m/company/ product- security/bull etins/august- 2021-bulletin	H-QUA-IPQ8- 170921/538
ipq8076			CVE ID : CVE-2021-1972		
1040070				F	
Out-of- bounds Read	08-Sep-21	3.6	Buffer over read could occur due to incorrect check of buffer size while flashing emmc devices in Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking CVE ID : CVE-2021-1928	https://www. qualcomm.co m/company/ product- security/bull etins/august- 2021-bulletin	H-QUA-IPQ8- 170921/539
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	08-Sep-21	10	Possible buffer overflow due to improper validation of device types during P2P search in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT,	https://www. qualcomm.co m/company/ product- security/bull etins/august- 2021-bulletin	H-QUA-IPQ8- 170921/540

0-1

1-2

5-6

6-7

7-8

8-9

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking CVE ID : CVE-2021-1972		
ipq8076a					
Out-of- bounds Read	08-Sep-21	3.6	Buffer over read could occur due to incorrect check of buffer size while flashing emmc devices in Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking CVE ID : CVE-2021-1928	https://www. qualcomm.co m/company/ product- security/bull etins/august- 2021-bulletin	H-QUA-IPQ8- 170921/541
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	08-Sep-21	10	Possible buffer overflow due to improper validation of device types during P2P search in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Woice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking CVE ID : CVE-2021-1972	https://www. qualcomm.co m/company/ product- security/bull etins/august- 2021-bulletin	H-QUA-IPQ8- 170921/542
ipq8078				1	1

0-1

1-2

2-3 3-4 4-5 Page 201 of 1474 6-7

7-8

8-9 9-10

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Out-of- bounds Read	08-Sep-21	3.6	Buffer over read could occur due to incorrect check of buffer size while flashing emmc devices in Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking	https://www. qualcomm.co m/company/ product- security/bull etins/august- 2021-bulletin	H-QUA-IPQ8- 170921/543
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	08-Sep-21	10	CVE ID : CVE-2021-1928 Possible buffer overflow due to improper validation of device types during P2P search in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Woice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking CVE ID : CVE-2021-1972	https://www. qualcomm.co m/company/ product- security/bull etins/august- 2021-bulletin	H-QUA-IPQ8- 170921/544
ipq8078a					
Out-of- bounds Read	08-Sep-21	3.6	Buffer over read could occur due to incorrect check of buffer size while flashing emmc devices in Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon	https://www. qualcomm.co m/company/ product- security/bull etins/august- 2021-bulletin	H-QUA-IPQ8- 170921/545

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Wired Infrastructure and Networking		
			0		
			CVE ID : CVE-2021-1928		
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	08-Sep-21	10	Possible buffer overflow due to improper validation of device types during P2P search in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Woice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking	https://www. qualcomm.co m/company/ product- security/bull etins/august- 2021-bulletin	H-QUA-IPQ8- 170921/546
			CVE ID : CVE-2021-1972		
ipq8173					
Out-of- bounds Read	08-Sep-21	3.6	Buffer over read could occur due to incorrect check of buffer size while flashing emmc devices in Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking CVE ID : CVE-2021-1928	https://www. qualcomm.co m/company/ product- security/bull etins/august- 2021-bulletin	H-QUA-IPQ8- 170921/547
Buffor Conv				https://www.	
Buffer Copy without Checking Size of Input ('Classic Buffer	08-Sep-21	10	Possible buffer overflow due to improper validation of device types during P2P search in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity,	https://www. qualcomm.co m/company/ product- security/bull etins/august-	H-QUA-IPQ8- 170921/548
CVSS Scoring Sca	ale 0-1	1-2	2-3 3-4 4-5 5-6	6-7 7-8	8-9 9-10

Page 203 of 1474

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Overflow')			Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking CVE ID : CVE-2021-1972	2021-bulletin	
ipq8174	L			I	
Out-of- bounds Read	08-Sep-21	3.6	Buffer over read could occur due to incorrect check of buffer size while flashing emmc devices in Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking	https://www. qualcomm.co m/company/ product- security/bull etins/august- 2021-bulletin	H-QUA-IPQ8- 170921/549
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	08-Sep-21	10	CVE ID : CVE-2021-1928 Possible buffer overflow due to improper validation of device types during P2P search in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer IOT, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Woice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking CVE ID : CVE-2021-1972	https://www. qualcomm.co m/company/ product- security/bull etins/august- 2021-bulletin	H-QUA-IPQ8- 170921/550

Weakness	Publish Date	CVSS	Description & CVE ID	Description & CVE ID Patch	
mdm8207		1			
Loop with Unreachable Exit Condition ('Infinite Loop')	08-Sep-21	5	Loop with unreachable exit condition may occur due to improper handling of unsupported input in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Voice & Music, Snapdragon Wearables CVE ID : CVE-2021-1914	https://www. qualcomm.co m/company/ product- security/bull etins/august- 2021-bulletin	H-QUA- MDM8- 170921/551
Out-of- bounds Write	08-Sep-21	10	Possible buffer underflow due to lack of check for negative indices values when processing user provided input in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Voice & Music, Snapdragon Wearables CVE ID : CVE-2021-1916	https://www. qualcomm.co m/company/ product- security/bull etins/august- 2021-bulletin	H-QUA- MDM8- 170921/552
Integer Underflow (Wrap or Wraparoun d)	08-Sep-21	10	Integer underflow can occur when the RTCP length is lesser than than the actual blocks present in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Voice & Music, Snapdragon Wearables	https://www. qualcomm.co m/company/ product- security/bull etins/august- 2021-bulletin	H-QUA- MDM8- 170921/553

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

0-1

1-2

2-3 3-4

4-5

6-7

5-6

7-8

8-9

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2021-1919		
Integer Underflow (Wrap or Wraparoun d)	08-Sep-21	10	Integer underflow can occur due to improper handling of incoming RTCP packets in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Voice & Music, Snapdragon Wearables CVE ID : CVE-2021-1920	https://www. qualcomm.co m/company/ product- security/bull etins/august- 2021-bulletin	H-QUA- MDM8- 170921/554
mdm8215					
Out-of- bounds Write	08-Sep-21	10	Possible buffer underflow due to lack of check for negative indices values when processing user provided input in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Voice & Music, Snapdragon Wearables CVE ID : CVE-2021-1916	https://www. qualcomm.co m/company/ product- security/bull etins/august- 2021-bulletin	H-QUA- MDM8- 170921/555
Integer Underflow (Wrap or Wraparoun d)	08-Sep-21	10	Integer underflow can occur due to improper handling of incoming RTCP packets in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Voice & Music, Snapdragon Wearables	https://www. qualcomm.co m/company/ product- security/bull etins/august- 2021-bulletin	H-QUA- MDM8- 170921/556
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 & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2021-1920		
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	08-Sep-21	10	Possible buffer overflow due to improper validation of device types during P2P search in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Woice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking	https://www. qualcomm.co m/company/ product- security/bull etins/august- 2021-bulletin	H-QUA- MDM8- 170921/557
			CVE ID : CVE-2021-1972		
mdm8215m					
Out-of- bounds Write	08-Sep-21	10	Possible buffer underflow due to lack of check for negative indices values when processing user provided input in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Voice & Music, Snapdragon Wearables CVE ID : CVE-2021-1916	https://www. qualcomm.co m/company/ product- security/bull etins/august- 2021-bulletin	H-QUA- MDM8- 170921/558
Integer Underflow (Wrap or Wraparoun d)	08-Sep-21	10	Integer underflow can occur due to improper handling of incoming RTCP packets in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT,	https://www. qualcomm.co m/company/ product- security/bull etins/august- 2021-bulletin	H-QUA- MDM8- 170921/559

0-1

1-2

5-6

6-7

7-8

8-9

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Snapdragon IoT, Snapdragon Voice & Music, Snapdragon Wearables CVE ID : CVE-2021-1920		
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	08-Sep-21	10	CVE ID : CVE-2021-1920Possible buffer overflow dueto improper validation ofdevice types during P2Psearch in Snapdragon Auto,Snapdragon Compute,Snapdragon Compute,Snapdragon Connectivity,Snapdragon Consumer IOT,Snapdragon Consumer IOT,Snapdragon Industrial IOT,Snapdragon Mobile,Snapdragon Wearables,Snapdragon WiredInfrastructure andNetworkingCVE ID : CVE-2021-1972	https://www. qualcomm.co m/company/ product- security/bull etins/august- 2021-bulletin	H-QUA- MDM8- 170921/560
mdm8615m				[
Out-of- bounds Write	08-Sep-21	10	Possible buffer underflow due to lack of check for negative indices values when processing user provided input in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Voice & Music, Snapdragon Wearables CVE ID : CVE-2021-1916	https://www. qualcomm.co m/company/ product- security/bull etins/august- 2021-bulletin	H-QUA- MDM8- 170921/561
Integer				1	
Integer Underflow (Wrap or Wraparoun d)	08-Sep-21	10	Integer underflow can occur due to improper handling of incoming RTCP packets in Snapdragon Auto, Snapdragon Compute,	https://www. qualcomm.co m/company/ product- security/bull	H-QUA- MDM8- 170921/562
CVSS Scoring Sc	ale 0-1	1-2	Snapdragon Compute,2-33-44-55-6Page 208 of 1474	security/bull6-77-8	8-9 9-10

Page 208 of 1474

Ruffer Copy without Checking Size of Input (Classic Buffer Copy without Checking Size of Input (Classic Burfer Overflow')Input Size of Input (Classic Burfer Copy (Size of Input (Classic Burfer Overflow')Input Size of Input (Classic Burfer Copy (Size of Input (Classic Burfer Overflow')Input Size of Input (Classic Burfer Overflow')Input Size of Input (Size of Input (Size of Input (Size of Input (Size of Input (Classic Burfer Overflow')Intpit Size of Input (Size of Input (S	Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Buffer Copy without Checking Size of Input (Classic Overflow')08-Sep-21IPossible buffer overflow due to improper validation of device types during P2P search in Snapdragon Conpute, Snapdragon Connectivity, Snapdragon Connectivity, Snapdragon Industrial IOT, Snapdragon Nobile, Snapdragon Wearables, Snapdragon Consumer IoT, Networkinghttps://www. this//www. qualcomm.co m/company/ product- scurity/bull etins/august- 2021-bulletinH-QUA- MDM8- 170921/563mam9150Exposure of Resource to Wrong Sphere08-Sep-212.1Child process can leak information from parent process due to numeric pids are getting compared and these pid can be reused in Snapdragon ConsumerioT, Snapdragon ConsumerioT, Snapdragon ConsumerioT, Snapdragon ConsumerioT, Snapdragon ConsumerioT, Snapdragon ConsumerioT, Snapdragon Mobile, Snapdragon Mobile, Snapdragon Mobile, Snapdragon Mobile, Snapdragon ConsumerioT, Snapdragon Mobile, Snapdragon Mobile,				Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Voice & Music, Snapdragon	, .	
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')Its and the second of t				CVE ID : CVE-2021-1920		
Exposure of Resource to Wrong Sphere08-Sep-212.1Child process can leak information from parent process due to numeric pids are getting compared and these pid can be reused in Snapdragon Auto, Snapdragon Connectivity, Snapdragon Connectivity, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wearableshttps://www. qualcomm.co m/company/ product- security/bull etins/august- 2021-bulletinH-QUA- MDM9- 170921/564	without Checking Size of Input ('Classic Buffer	08-Sep-21	10	to improper validation of device types during P2P search in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Woice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking	qualcomm.co m/company/ product- security/bull etins/august-	MDM8-
Exposure of Resource to Wrong Sphere08-Sep-212.1information from parent process due to numeric pids are getting compared and these pid can be reused in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wearableshttps://www. qualcomm.co m/company/ product- security/bull etins/august- 2021-bulletinH-QUA- MDM9- 170921/564	mdm9150				I	
Loop with08-Sep-215Loop with unreachable exithttps://www.H-QUA-	Resource to Wrong	08-Sep-21	2.1	information from parent process due to numeric pids are getting compared and these pid can be reused in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wearables	qualcomm.co m/company/ product- security/bull etins/august-	MDM9-
	Loop with	08-Sep-21	5	Loop with unreachable exit	https://www.	H-QUA-

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID			
Unreachable Exit Condition ('Infinite Loop')			condition may occur due to improper handling of unsupported input in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Voice & Music, Snapdragon Wearables	qualcomm.co m/company/ product- security/bull etins/august- 2021-bulletin	MDM9- 170921/565			
			CVE ID : CVE-2021-1914					
Out-of- bounds Write	08-Sep-21	10	Possible buffer underflow due to lack of check for negative indices values when processing user provided input in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Voice & Music, Snapdragon Wearables	https://www. qualcomm.co m/company/ product- security/bull etins/august- 2021-bulletin	H-QUA- MDM9- 170921/566			
			CVE ID : CVE-2021-1916					
Integer Underflow (Wrap or Wraparoun d)	08-Sep-21	10	Integer underflow can occur when the RTCP length is lesser than than the actual blocks present in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Voice & Music, Snapdragon Wearables CVE ID : CVE-2021-1919	https://www. qualcomm.co m/company/ product- security/bull etins/august- 2021-bulletin	H-QUA- MDM9- 170921/567			
Integer	08-Sep-21	10	Integer underflow can occur	https://www.	H-QUA-			
Integer 00-3cp-21 Integer underflow can occur https://www. H-QUA-								

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Underflow (Wrap or Wraparoun d)			due to improper handling of incoming RTCP packets in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Voice & Music, Snapdragon Wearables CVE ID : CVE-2021-1920	qualcomm.co m/company/ product- security/bull etins/august- 2021-bulletin	MDM9- 170921/568
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	08-Sep-21	10	Possible buffer overflow due to improper validation of device types during P2P search in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Woice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking CVE ID : CVE-2021-1972	https://www. qualcomm.co m/company/ product- security/bull etins/august- 2021-bulletin	H-QUA- MDM9- 170921/569
mdm9205	I			I	
Loop with Unreachable Exit Condition ('Infinite Loop')	08-Sep-21	5	Loop with unreachable exit condition may occur due to improper handling of unsupported input in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Voice & Music, Snapdragon	https://www. qualcomm.co m/company/ product- security/bull etins/august- 2021-bulletin	H-QUA- MDM9- 170921/570

CVSS Scoring Scale	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10
			Р	age 211 c	of 1474					

Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
		Wearables CVE ID : CVE-2021-1914		
08-Sep-21	10	Possible buffer underflow due to lack of check for negative indices values when processing user provided input in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Voice & Music, Snapdragon Wearables	https://www. qualcomm.co m/company/ product- security/bull etins/august- 2021-bulletin	H-QUA- MDM9- 170921/571
		CVE ID : CVE-2021-1916		
08-Sep-21	10	Integer underflow can occur due to improper handling of incoming RTCP packets in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Voice & Music, Snapdragon Wearables CVE ID : CVE-2021-1920	https://www. qualcomm.co m/company/ product- security/bull etins/august- 2021-bulletin	H-QUA- MDM9- 170921/572
Exposure of Resource to Wrong Sphere 08-Sep-21 2.1		Child process can leak information from parent process due to numeric pids are getting compared and these pid can be reused in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT,	https://www. qualcomm.co m/company/ product- security/bull etins/august- 2021-bulletin	H-QUA- MDM9- 170921/573
	08-Sep-21	08-Sep-21 10 08-Sep-21 10 08-Sep-21 10 08-Sep-21 10	Image: constraint of the second sec	08-Sep-2110Wearables CVE ID : CVE-2021-1914Https://www. qualcomm.co mcompany/ product- snapdragon Conpute, Snapdragon Consumer 10T, Snapdragon Industrial 10T, Snapdragon Compute, Snapdragon Industrial 10T, Snapdragon Industrial

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables CVE ID : CVE-2021-1904		
Loop with Unreachable Exit Condition ('Infinite Loop')	08-Sep-21	5	Loop with unreachable exit condition may occur due to improper handling of unsupported input in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Voice & Music, Snapdragon Wearables	https://www. qualcomm.co m/company/ product- security/bull etins/august- 2021-bulletin	H-QUA- MDM9- 170921/574
Out-of- bounds Write	08-Sep-21	10	CVE ID : CVE-2021-1914 Possible buffer underflow due to lack of check for negative indices values when processing user provided input in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Voice & Music, Snapdragon Wearables CVE ID : CVE-2021-1916	https://www. qualcomm.co m/company/ product- security/bull etins/august- 2021-bulletin	H-QUA- MDM9- 170921/575
Integer Underflow (Wrap or Wraparoun d)	08-Sep-21	10	Integer underflow can occur when the RTCP length is lesser than than the actual blocks present in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT,	https://www. qualcomm.co m/company/ product- security/bull etins/august- 2021-bulletin	H-QUA- MDM9- 170921/576

1-2

0-1

6-7

5-6

7-8

8-9

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Snapdragon IoT, Snapdragon Voice & Music, Snapdragon Wearables		
			CVE ID : CVE-2021-1919		
Integer Underflow (Wrap or Wraparoun d)	08-Sep-21	10	Integer underflow can occur due to improper handling of incoming RTCP packets in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Voice & Music, Snapdragon Wearables	https://www. qualcomm.co m/company/ product- security/bull etins/august- 2021-bulletin	H-QUA- MDM9- 170921/577
			CVE ID : CVE-2021-1920 Buffer over read could occur		
Out-of- bounds Read	08-Sep-21	3.6	due to incorrect check of buffer size while flashing emmc devices in Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking	https://www. qualcomm.co m/company/ product- security/bull etins/august- 2021-bulletin	H-QUA- MDM9- 170921/578
			CVE ID : CVE-2021-1928		
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	08-Sep-21	10	Possible buffer overflow due to improper validation of device types during P2P search in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile,	https://www. qualcomm.co m/company/ product- security/bull etins/august- 2021-bulletin	H-QUA- MDM9- 170921/579

0-1 1-2

6-7

5-6

7-8

8-9

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking CVE ID : CVE-2021-1972		
mdm9207					
Loop with Unreachable Exit Condition ('Infinite Loop')	08-Sep-21	5	Loop with unreachable exit condition may occur due to improper handling of unsupported input in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Voice & Music, Snapdragon Wearables CVE ID : CVE-2021-1914	https://www. qualcomm.co m/company/ product- security/bull etins/august- 2021-bulletin	H-QUA- MDM9- 170921/580
Out-of- bounds Write	08-Sep-21	10	Possible buffer underflow due to lack of check for negative indices values when processing user provided input in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Voice & Music, Snapdragon Wearables CVE ID : CVE-2021-1916	https://www. qualcomm.co m/company/ product- security/bull etins/august- 2021-bulletin	H-QUA- MDM9- 170921/581
Integer Underflow (Wrap or Wraparoun d)	08-Sep-21	10	Integer underflow can occur when the RTCP length is lesser than than the actual blocks present in Snapdragon Auto, Snapdragon Compute,	https://www. qualcomm.co m/company/ product- security/bull	H-QUA- MDM9- 170921/582
CVSS Scoring Scale 0-1 1-2 2-3 3-4 4-5 5-6 6-7 7-8 8-9 9-10 Page 215 of 1474					

Page 215 of 1474

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Voice & Music, Snapdragon Wearables	etins/august- 2021-bulletin	
			CVE ID : CVE-2021-1919		
Integer Underflow (Wrap or Wraparoun d)	08-Sep-21	10	Integer underflow can occur due to improper handling of incoming RTCP packets in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Voice & Music, Snapdragon Wearables	https://www. qualcomm.co m/company/ product- security/bull etins/august- 2021-bulletin	H-QUA- MDM9- 170921/583
			CVE ID : CVE-2021-1920		
mdm9215				1	1
Out-of- bounds Write	08-Sep-21	10	Possible buffer underflow due to lack of check for negative indices values when processing user provided input in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Voice & Music, Snapdragon Wearables CVE ID : CVE-2021-1916	https://www. qualcomm.co m/company/ product- security/bull etins/august- 2021-bulletin	H-QUA- MDM9- 170921/584
Integer Underflow (Wrap or Wraparoun d)	08-Sep-21	10	Integer underflow can occur due to improper handling of incoming RTCP packets in Snapdragon Auto, Snapdragon Compute,	https://www. qualcomm.co m/company/ product- security/bull	H-QUA- MDM9- 170921/585
CVSS Scoring Scale 0-1 1-2 2-3 3-4 4-5 5-6 6-7 7-8 8-9 9-10 Page 216 of 1474					

Page 216 of 1474

	CVSS	Description & CVE ID	Patch	NCIIPC ID
		Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Voice & Music, Snapdragon Wearables	etins/august- 2021-bulletin	
		CVE ID : CVE-2021-1920		
08-Sep-21	10	Possible buffer overflow due to improper validation of device types during P2P search in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Woice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking CVE ID : CVE-2021-1972	https://www. qualcomm.co m/company/ product- security/bull etins/august- 2021-bulletin	H-QUA- MDM9- 170921/586
08-Sep-21	 Possible buffer underflow due to lack of check for negative indices values when processing user provided input in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Voice & Music, Snapdragon Wearables CVE ID : CVE-2021-1916 		https://www. qualcomm.co m/company/ product- security/bull etins/august- 2021-bulletin	H-QUA- MDM9- 170921/587
		Integer underflow can occur	https://www.	H-QUA-
			08-Sep-21IOSnapdragon Consumer IOT, Snapdragon IoT, Snapdragon Voice & Music, Snapdragon Voice & Music, Snapdragon Wearables08-Sep-21IOPossible buffer overflow due to improper validation of device types during P2P search in Snapdragon Auto, Snapdragon Conpute, Snapdragon Consumer IOT, Snapdragon Consumer IOT, Snapdragon Consumer IOT, Snapdragon Nobile, Snapdragon Wearables, Snapdragon Wearables, Snapdragon Wired Infrastructure and NetworkingCVE ID : CVE-2021-197208-Sep-21IOSnapdragon Consumer IOT, Snapdragon Wired Infrastructure and NetworkingDPossible buffer underflow due to lack of check for negative indices values when processing user provided input in Snapdragon Auto, Snapdragon Consumer IOT, Snapdragon Consumer IOT, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Consumer IOT, Snapdragon Consumer IOT, Snapdragon Consumer IOT, Snapdragon Consumer IOT, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Industria	08-Sep-2110Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Wearables2021-bulletin08-Sep-2110Possible buffer overflow due to improper validation of device types during P2P search in Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Consumer IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Viered Infrastructure and Networkinghttps://www. qualcomm.co m/company/ product- security/bull etins/august- 2021-bulletin08-Sep-2110Possible buffer underflow due to lack of check for negative indices values when processing user provided input in Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Consumer IOT, Snapdragon Consumer IOT, Snapdragon Industrial

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
(Wrap or Wraparoun d)			incoming RTCP packets in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Voice & Music, Snapdragon Wearables CVE ID : CVE-2021-1920	m/company/ product- security/bull etins/august- 2021-bulletin	170921/588
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	08-Sep-21	10	Possible buffer overflow due to improper validation of device types during P2P search in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Woice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking CVE ID : CVE-2021-1972	https://www. qualcomm.co m/company/ product- security/bull etins/august- 2021-bulletin	H-QUA- MDM9- 170921/589
mdm9250					
Exposure of Resource to Wrong Sphere	08-Sep-21	2.1	Child process can leak information from parent process due to numeric pids are getting compared and these pid can be reused in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music,	https://www. qualcomm.co m/company/ product- security/bull etins/august- 2021-bulletin	H-QUA- MDM9- 170921/590

CVSS Scoring Scale	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10	
Page 218 of 1474											

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Snapdragon Wearables		
			CVE ID : CVE-2021-1904		
Loop with Unreachable Exit Condition ('Infinite Loop')	08-Sep-21	5	Loop with unreachable exit condition may occur due to improper handling of unsupported input in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Voice & Music, Snapdragon Wearables CVE ID : CVE-2021-1914	https://www. qualcomm.co m/company/ product- security/bull etins/august- 2021-bulletin	H-QUA- MDM9- 170921/591
Out-of- bounds Write	08-Sep-21	10	Possible buffer underflow due to lack of check for negative indices values when processing user provided input in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Voice & Music, Snapdragon Wearables CVE ID : CVE-2021-1916	https://www. qualcomm.co m/company/ product- security/bull etins/august- 2021-bulletin	H-QUA- MDM9- 170921/592
Integer Underflow (Wrap or Wraparoun d)	08-Sep-21	10	Integer underflow can occur when the RTCP length is lesser than than the actual blocks present in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Voice & Music, Snapdragon	https://www. qualcomm.co m/company/ product- security/bull etins/august- 2021-bulletin	H-QUA- MDM9- 170921/593

0-1

1-2

2-3 3-4 4-5 Page 219 of 1474 6-7

5-6

7-8

8-9

Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
		Wearables		
		CVE ID : CVE-2021-1919		
08-Sep-21	10	Integer underflow can occur due to improper handling of incoming RTCP packets in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Voice & Music, Snapdragon Wearables	https://www. qualcomm.co m/company/ product- security/bull etins/august- 2021-bulletin	H-QUA- MDM9- 170921/594
		CVE ID : CVE-2021-1920		
08-Sep-21	10	Possible buffer overflow due to improper validation of device types during P2P search in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Woice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking CVE ID : CVE-2021-1972	https://www. qualcomm.co m/company/ product- security/bull etins/august- 2021-bulletin	H-QUA- MDM9- 170921/595
08-Sep-21	10	Possible buffer underflow due to lack of check for negative indices values when processing user provided input in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT,	https://www. qualcomm.co m/company/ product- security/bull etins/august- 2021-bulletin	H-QUA- MDM9- 170921/596
	08-Sep-21		08-Sep-21CVE ID : CVE-2021-191908-Sep-21Integer underflow can occur due to improper handling of incoming RTCP packets in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Industrial IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Voice & Music, Snapdragon Industrial IOT, Snapdragon Compute, Snapdragon Compute, Snapdragon Consumer IOT, Snapdragon Consumer IOT, Snapdragon Consumer IOT, Snapdragon Consumer IOT, Snapdragon Consumer IOT, Snapdragon Consumer IOT, Snapdragon Mobile, Snapdragon Mobile, Snapdragon Wierd Infrastructure and Networking08-Sep-21Possible buffer underflow due to lack of check for negative indices values when processing user provided input in Snapdragon Auto, Snapdragon Compute, Snapdragon Compute, Snapdragon Compute, Snapdragon Compute, Snapdragon Compute, Snapdragon Compute, Snapdragon Wierd Infrastructure and Networking	O8-Sep-21Integer underflow can occur due to improper handling of incoming RTCP packets in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Industrial IOT, Snapdragon Industrial IOT, Snapdragon Industrial IOT, Snapdragon Iot, Snapdragon Voice & Music, Snapdragon Voice & Music, Snapdragon Auto, Snapdragon Consumer IOT, Snapdragon Iot, Snapdragon Voice & Music, Snapdragon Voice & Music, Snapdragon Auto, Snapdragon Consumer IOT, Snapdragon Consumer IOT, Snapdragon Consumer IOT, Snapdragon Compute, Snapdragon Consumer IOT, Snapdragon Voice & Music, Snapdragon Wired Infrastructure and Networkinghttps://www. qualcomm.co m/company/

Page 220 of 1474

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Voice & Music, Snapdragon Wearables		
			CVE ID : CVE-2021-1916		
Integer Underflow (Wrap or Wraparoun d)	08-Sep-21	10	Integer underflow can occur due to improper handling of incoming RTCP packets in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Voice & Music, Snapdragon Wearables CVE ID : CVE-2021-1920	https://www. qualcomm.co m/company/ product- security/bull etins/august- 2021-bulletin	H-QUA- MDM9- 170921/597
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	08-Sep-21	10	Possible buffer overflow due to improper validation of device types during P2P search in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Woice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking CVE ID : CVE-2021-1972	https://www. qualcomm.co m/company/ product- security/bull etins/august- 2021-bulletin	H-QUA- MDM9- 170921/598
mdm9330					
Out-of- bounds Write	08-Sep-21	10	Possible buffer underflow due to lack of check for negative indices values when processing user provided input in Snapdragon Auto,	https://www. qualcomm.co m/company/ product- security/bull	H-QUA- MDM9- 170921/599
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 & CVE ID	Patch	NCIIPC ID					
			Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Voice & Music, Snapdragon Wearables	etins/august- 2021-bulletin						
			CVE ID : CVE-2021-1916							
Integer Underflow (Wrap or Wraparoun d)	08-Sep-21	10	Integer underflow can occur due to improper handling of incoming RTCP packets in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Voice & Music, Snapdragon Wearables	https://www. qualcomm.co m/company/ product- security/bull etins/august- 2021-bulletin	H-QUA- MDM9- 170921/600					
			CVE ID : CVE-2021-1920							
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	08-Sep-21	10	Possible buffer overflow due to improper validation of device types during P2P search in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Woice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking CVE ID : CVE-2021-1972	https://www. qualcomm.co m/company/ product- security/bull etins/august- 2021-bulletin	H-QUA- MDM9- 170921/601					
mdm9607	mdm9607									
Exposure of	08-Sep-21	2.1	Child process can leak	https://www.	H-QUA-					
Resource to			information from parent	qualcomm.co	MDM9-					
CVSS Scoring Sc	ale 0-1	1-2	2-3 3-4 4-5 5-6 Page 222 of 1474	6-7 7-8	8-9 <mark>9-10</mark>					

Page 222 of 1474

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Wrong Sphere			process due to numeric pids are getting compared and these pid can be reused in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wearables CVE ID : CVE-2021-1904	m/company/ product- security/bull etins/august- 2021-bulletin	170921/602
Loop with Unreachable Exit Condition ('Infinite Loop')	08-Sep-21	5	Loop with unreachable exit condition may occur due to improper handling of unsupported input in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Voice & Music, Snapdragon Wearables CVE ID : CVE-2021-1914	https://www. qualcomm.co m/company/ product- security/bull etins/august- 2021-bulletin	H-QUA- MDM9- 170921/603
Out-of- bounds Write	08-Sep-21	10	Possible buffer underflow due to lack of check for negative indices values when processing user provided input in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Voice & Music, Snapdragon Wearables CVE ID : CVE-2021-1916	https://www. qualcomm.co m/company/ product- security/bull etins/august- 2021-bulletin	H-QUA- MDM9- 170921/604

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
Integer Underflow (Wrap or Wraparoun d)	08-Sep-21	10	Integer underflow can occurwhen the RTCP length islesser than than the actualblocks present in SnapdragonAuto, Snapdragon Compute,Snapdragon Connectivity,Snapdragon Consumer IOT,Snapdragon Industrial IOT,Snapdragon IoT, SnapdragonVoice & Music, SnapdragonWearablesCVE ID : CVE-2021-1919		H-QUA- MDM9- 170921/605
Integer Underflow (Wrap or Wraparoun d)	08-Sep-21	10	Integer underflow can occur due to improper handling of incoming RTCP packets in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Voice & Music, Snapdragon Wearables CVE ID : CVE-2021-1920	https://www. qualcomm.co m/company/ product- security/bull etins/august- 2021-bulletin	H-QUA- MDM9- 170921/606
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	08-Sep-21	10	Possible buffer overflow due to improper validation of device types during P2P search in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Woice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking	https://www. qualcomm.co m/company/ product- security/bull etins/august- 2021-bulletin	H-QUA- MDM9- 170921/607

CVSS Scoring Scale	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10	
	Page 224 of 1474										

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2021-1972		
mdm9615					
Out-of- bounds Write	08-Sep-21	10	Possible buffer underflow due to lack of check for negative indices values when processing user provided input in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Voice & Music, Snapdragon Wearables CVE ID : CVE-2021-1916	https://www. qualcomm.co m/company/ product- security/bull etins/august- 2021-bulletin	H-QUA- MDM9- 170921/608
Integer Underflow (Wrap or Wraparoun d)	08-Sep-21	10	Integer underflow can occur due to improper handling of incoming RTCP packets in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Voice & Music, Snapdragon Wearables CVE ID : CVE-2021-1920	https://www. qualcomm.co m/company/ product- security/bull etins/august- 2021-bulletin	H-QUA- MDM9- 170921/609
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	08-Sep-21	10	Possible buffer overflow due to improper validation of device types during P2P search in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables,	https://www. qualcomm.co m/company/ product- security/bull etins/august- 2021-bulletin	H-QUA- MDM9- 170921/610

0-1

1-2 2-3 4-5

6-7

5-6

7-8

8-9

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Snapdragon Wired Infrastructure and Networking		
			CVE ID : CVE-2021-1972		
mdm9615m					
Out-of- bounds Write	08-Sep-21	10	Possible buffer underflow due to lack of check for negative indices values when processing user provided input in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Voice & Music, Snapdragon Wearables CVE ID : CVE-2021-1916	https://www. qualcomm.co m/company/ product- security/bull etins/august- 2021-bulletin	H-QUA- MDM9- 170921/611
Integer Underflow (Wrap or Wraparoun d)	08-Sep-21	10	Integer underflow can occur due to improper handling of incoming RTCP packets in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Voice & Music, Snapdragon Wearables CVE ID : CVE-2021-1920	https://www. qualcomm.co m/company/ product- security/bull etins/august- 2021-bulletin	H-QUA- MDM9- 170921/612
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	08-Sep-21	10	Possible buffer overflow due to improper validation of device types during P2P search in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT,	https://www. qualcomm.co m/company/ product- security/bull etins/august- 2021-bulletin	H-QUA- MDM9- 170921/613
CVSS Scoring Sc	ale 0-1	1-2	2-3 3-4 4-5 5-6	6-7 7-8	8-9 9-10

 3-4
 4-5

 Page 226 of 1474

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking		
			CVE ID : CVE-2021-1972		
mdm9625	I			I	L
Out-of- bounds Write	08-Sep-21	10	Possible buffer underflow due to lack of check for negative indices values when processing user provided input in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Voice & Music, Snapdragon Wearables CVE ID : CVE-2021-1916	https://www. qualcomm.co m/company/ product- security/bull etins/august- 2021-bulletin	H-QUA- MDM9- 170921/614
Integer Underflow (Wrap or Wraparoun d)	08-Sep-21	10	Integer underflow can occur when the RTCP length is lesser than than the actual blocks present in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Voice & Music, Snapdragon Wearables CVE ID : CVE-2021-1919	https://www. qualcomm.co m/company/ product- security/bull etins/august- 2021-bulletin	H-QUA- MDM9- 170921/615
Integer Underflow (Wrap or Wraparoun d)	08-Sep-21	10	Integer underflow can occur due to improper handling of incoming RTCP packets in Snapdragon Auto, Snapdragon Compute,	https://www. qualcomm.co m/company/ product- security/bull	H-QUA- MDM9- 170921/616

Page 227 of 1474

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Voice & Music, Snapdragon Wearables	etins/august- 2021-bulletin	
			CVE ID : CVE-2021-1920		
mdm9626				l	
Exposure of Resource to Wrong Sphere	08-Sep-21	2.1	Child process can leak information from parent process due to numeric pids are getting compared and these pid can be reused in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables CVE ID : CVE-2021-1904	https://www. qualcomm.co m/company/ product- security/bull etins/august- 2021-bulletin	H-QUA- MDM9- 170921/617
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	08-Sep-21	10	Possible buffer overflow due to improper validation of device types during P2P search in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Woice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking CVE ID : CVE-2021-1972	https://www. qualcomm.co m/company/ product- security/bull etins/august- 2021-bulletin	H-QUA- MDM9- 170921/618
mdm9628				1	1
CVSS Scoring Sc	ale 0-1	1-2	2-3 3-4 4-5 5-6 Page 228 of 1474	6-7 7-8	8-9 9-10

Exposure of Resource to Wrong Sphere08-Sep-212.1Child process can leak information from parent process due to numeric pids are getting compared and these pid can be reused in Snapdragon Conneutivity, Snapdragon Consumer 107, Snapdragon Consumer 107, Snapdragon Ocnestwirty, Snapdragon Wearableshttps://www. qualcomm.co m/company/ product- security/bull etins/august- 2021-bulletinH-QUA- MDM9- 170921/619Loop with Unreachable Exit Condition (Infinite Loop)08-Sep-215Songdragon Consumer 107, Snapdragon Consumer 107, Snapdragon Consumer 107, Snapdragon Industrial 107, Snapdragon Industri	Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Loop with Unreachable Exit Condition ('Infinite Loop')08-Sep-215condition may occur due to improper handling of unsupported input in Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon WearablesH-QUA- MDM9- 170921/620Out-of- bounds Write08-Sep-2110Possible buffer underflow due to lack of check for negative indices values when processing user provided input in Snapdragon Auto, Snapdragon Consumer IOT, Snapdragon Consumer IOT, Snapdragon Consumer IOT, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Consumer IOT, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Consumer IOT, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snap	Resource to Wrong	08-Sep-21	2.1	information from parent process due to numeric pids are getting compared and these pid can be reused in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wearables	qualcomm.co m/company/ product- security/bull etins/august-	MDM9-
Out-of- bounds08-Sep-2110due to lack of check for negative indices values when processing user provided input in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragonhttps://www. qualcomm.co m/company/ product- security/bull etins/august- 2021-bulletinH-QUA- MDM9- 170921/621	Unreachable Exit Condition ('Infinite	08-Sep-21	5	condition may occur due to improper handling of unsupported input in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Voice & Music, Snapdragon Wearables	qualcomm.co m/company/ product- security/bull etins/august-	MDM9-
	bounds	08-Sep-21	10	due to lack of check for negative indices values when processing user provided input in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Voice & Music, Snapdragon	qualcomm.co m/company/ product- security/bull etins/august-	MDM9-

Page 229 of 1474

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2021-1916		
Integer Underflow (Wrap or Wraparoun d)	08-Sep-21	10	Integer underflow can occur when the RTCP length is lesser than than the actual blocks present in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Voice & Music, Snapdragon Wearables CVE ID : CVE-2021-1919	https://www. qualcomm.co m/company/ product- security/bull etins/august- 2021-bulletin	H-QUA- MDM9- 170921/622
Integer Underflow (Wrap or Wraparoun d)	08-Sep-21	10	Integer underflow can occur due to improper handling of incoming RTCP packets in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Voice & Music, Snapdragon Wearables CVE ID : CVE-2021-1920	https://www. qualcomm.co m/company/ product- security/bull etins/august- 2021-bulletin	H-QUA- MDM9- 170921/623
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	08-Sep-21	10	Possible buffer overflow due to improper validation of device types during P2P search in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Woice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and	https://www. qualcomm.co m/company/ product- security/bull etins/august- 2021-bulletin	H-QUA- MDM9- 170921/624

CVSS Scoring Scale	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10
			P	age 230 c	of 1474					

	08-Sep-21		Networking CVE ID : CVE-2021-1972 Possible buffer underflow due to lack of check for negative indices values when processing user provided		
Out-of- bounds 0	08-Sep-21		Possible buffer underflow due to lack of check for negative indices values when		
Out-of- bounds 0	08-Sep-21		due to lack of check for negative indices values when		
bounds 0	08-Sep-21		due to lack of check for negative indices values when		
Write		10	input in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Voice & Music, Snapdragon Wearables	https://www. qualcomm.co m/company/ product- security/bull etins/august- 2021-bulletin	H-QUA- MDM9- 170921/625
			CVE ID : CVE-2021-1916		
Integer Underflow (Wrap or 0 Wraparoun d)	08-Sep-21	10	Integer underflow can occur due to improper handling of incoming RTCP packets in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Voice & Music, Snapdragon Wearables CVE ID : CVE-2021-1920	https://www. qualcomm.co m/company/ product- security/bull etins/august- 2021-bulletin	H-QUA- MDM9- 170921/626
Buffer Copy without Checking Size of Input 0 ('Classic Buffer Overflow')	08-Sep-21	10	Possible buffer overflow due to improper validation of device types during P2P search in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music,	https://www. qualcomm.co m/company/ product- security/bull etins/august- 2021-bulletin	H-QUA- MDM9- 170921/627
CVSS Scoring Scale	e 0-1	1-2	2-3 3-4 4-5 5-6	6-7 7-8	8-9 9-10

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking		
			CVE ID : CVE-2021-1972		
mdm9635m					
Out-of- bounds Write	08-Sep-21	10	Possible buffer underflow due to lack of check for negative indices values when processing user provided input in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Voice & Music, Snapdragon Wearables CVE ID : CVE-2021-1916	https://www. qualcomm.co m/company/ product- security/bull etins/august- 2021-bulletin	H-QUA- MDM9- 170921/628
Integer Underflow (Wrap or Wraparoun d)	08-Sep-21	10	Integer underflow can occur when the RTCP length is lesser than than the actual blocks present in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Voice & Music, Snapdragon Wearables CVE ID : CVE-2021-1919	https://www. qualcomm.co m/company/ product- security/bull etins/august- 2021-bulletin	H-QUA- MDM9- 170921/629
Integer Underflow (Wrap or Wraparoun d)	08-Sep-21	10	Integer underflow can occur due to improper handling of incoming RTCP packets in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT,	https://www. qualcomm.co m/company/ product- security/bull etins/august- 2021-bulletin	H-QUA- MDM9- 170921/630

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID		
			Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Voice & Music, Snapdragon Wearables				
			CVE ID : CVE-2021-1920				
mdm9640							
Exposure of Resource to Wrong Sphere	08-Sep-21	2.1	Child process can leak information from parent process due to numeric pids are getting compared and these pid can be reused in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables CVE ID : CVE-2021-1904	https://www. qualcomm.co m/company/ product- security/bull etins/august- 2021-bulletin	H-QUA- MDM9- 170921/631		
Loop with Unreachable Exit Condition ('Infinite Loop')	08-Sep-21	5	Loop with unreachable exit condition may occur due to improper handling of unsupported input in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Voice & Music, Snapdragon Wearables CVE ID : CVE-2021-1914	https://www. qualcomm.co m/company/ product- security/bull etins/august- 2021-bulletin	H-QUA- MDM9- 170921/632		
Out-of- bounds Write	08-Sep-21	10	Possible buffer underflow due to lack of check for negative indices values when processing user provided input in Snapdragon Auto,	https://www. qualcomm.co m/company/ product- security/bull	H-QUA- MDM9- 170921/633		
CVSS Scoring Sc	ale 0-1	1-2	2-3 3-4 4-5 5-6	6-7 7-8	8-9 9-10		

Page 233 of 1474

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Voice & Music, Snapdragon Wearables	etins/august- 2021-bulletin	
			CVE ID : CVE-2021-1916		
Integer Underflow (Wrap or Wraparoun d)	08-Sep-21	10	Integer underflow can occur when the RTCP length is lesser than than the actual blocks present in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Voice & Music, Snapdragon Wearables	https://www. qualcomm.co m/company/ product- security/bull etins/august- 2021-bulletin	H-QUA- MDM9- 170921/634
			CVE ID : CVE-2021-1919		
Integer Underflow (Wrap or Wraparoun d)	08-Sep-21	10	Integer underflow can occur due to improper handling of incoming RTCP packets in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Voice & Music, Snapdragon Wearables	https://www. qualcomm.co m/company/ product- security/bull etins/august- 2021-bulletin	H-QUA- MDM9- 170921/635
			CVE ID : CVE-2021-1920		
Buffer Copy without Checking Size of Input ('Classic Buffer	08-Sep-21	10	Possible buffer overflow due to improper validation of device types during P2P search in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity,	https://www. qualcomm.co m/company/ product- security/bull etins/august-	H-QUA- MDM9- 170921/636

0-1

1-2

4-5

5-6

6-7

7-8

8-9

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Overflow')			Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking CVE ID : CVE-2021-1972	2021-bulletin	
mdm9645	<u> </u>			<u> </u>	<u> </u>
Out-of- bounds Write	08-Sep-21	10	Possible buffer underflow due to lack of check for negative indices values when processing user provided input in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Voice & Music, Snapdragon Wearables	https://www. qualcomm.co m/company/ product- security/bull etins/august- 2021-bulletin	H-QUA- MDM9- 170921/637
Integer Underflow (Wrap or Wraparoun d)	08-Sep-21	10	CVE ID : CVE-2021-1916 Integer underflow can occur when the RTCP length is lesser than than the actual blocks present in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Voice & Music, Snapdragon Wearables CVE ID : CVE-2021-1919	https://www. qualcomm.co m/company/ product- security/bull etins/august- 2021-bulletin	H-QUA- MDM9- 170921/638
Integer Underflow (Wrap or	08-Sep-21	10	Integer underflow can occur due to improper handling of incoming RTCP packets in	https://www. qualcomm.co m/company/	H-QUA- MDM9- 170921/639
CVSS Scoring Sc	ale 0-1	1-2	2-3 3-4 4-5 5-6	6-7 7-8	8-9 9-10

Wraparoun d)Wraparoun d)Image: Subscript of the s	Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Exposure of Resource to Wrong Sphere08-Sep-212.1Child process can leak information from parent process due to numeric pids are getting compared and these pid can be reused in Snapdragon Auto, Snapdragon Consumer IOT, Snapdragon Consumer IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Voice & Music, Snapdragon Voice & Music, Snapdragon Voice & Music, Snapdragon Consumer IOT, Snapdragon Voice & Music, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Voice & Music, Snapdragon Consumer IOT, Snapdragon Voice & Music, Snapdragon Consumer IOT, Snapdragon Voice & Music, Snapdragon Nobile, Snapdragon Voice & Music, Snapdragon Voice & Music, Snapdragon Voice & Music, Snapdragon Mobile, Snapdragon Nobile, Snapdragon Voice & Music, Snapdragon Nobile, Snapdragon Compute, Snapdragon Consumer IOT, Snapdragon Industrial I	-			Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Voice & Music, Snapdragon Wearables	security/bull etins/august-	
Exposure of Resource to Wrong Spheree.s.information from parent process due to numeric pids are getting compared and these pid can be reused in Snapdragon Compute, Snapdragon Consumer IOT, Snapdragon Mobile, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon WearablesH-QUA- MDM9- 170921/640Loop with Unreachable Exit Condition (Infinite Loop')8-Sep-215Song With unreachable exit condition may occur due to improper handling of 	mdm9650					
Loop with Unreachable Exit ConditionNapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Voice & Music, Snapdragon Voice WearablesH-QUA- MDM9- 170921/641CVE ID : CVE-2021-1914Unit Industrial IOT, Unit Industrial IOT, Unit Industrial IOT, Unit IDT, Unit I	Resource to Wrong	08-Sep-21	2.1	information from parent process due to numeric pids are getting compared and these pid can be reused in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wearables	qualcomm.co m/company/ product- security/bull etins/august-	MDM9-
Out-of-08-Sep-2110Possible buffer underflowhttps://www.H-QUA-	Unreachable Exit Condition ('Infinite	08-Sep-21	5	condition may occur due to improper handling of unsupported input in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Voice & Music, Snapdragon Wearables	qualcomm.co m/company/ product- security/bull etins/august-	MDM9-
	Out-of-	08-Sep-21	10	Possible buffer underflow	https://www.	H-QUA-

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
bounds Write			due to lack of check for negative indices values when processing user provided input in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Voice & Music, Snapdragon Wearables CVE ID : CVE-2021-1916	qualcomm.co m/company/ product- security/bull etins/august- 2021-bulletin	MDM9- 170921/642
Integer Underflow (Wrap or Wraparoun d)	08-Sep-21	10	Integer underflow can occur when the RTCP length is lesser than than the actual blocks present in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Voice & Music, Snapdragon Wearables CVE ID : CVE-2021-1919	https://www. qualcomm.co m/company/ product- security/bull etins/august- 2021-bulletin	H-QUA- MDM9- 170921/643
Integer Underflow (Wrap or Wraparoun d)	08-Sep-21	10	Integer underflow can occur due to improper handling of incoming RTCP packets in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Voice & Music, Snapdragon Wearables CVE ID : CVE-2021-1920	https://www. qualcomm.co m/company/ product- security/bull etins/august- 2021-bulletin	H-QUA- MDM9- 170921/644
Buffer Copy without	08-Sep-21	10	Possible buffer overflow due to improper validation of	https://www. qualcomm.co	H-QUA- MDM9-

CVSS Scoring Scale	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10
			р	aga 227 g	f 1 / 7 /					

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Checking Size of Input ('Classic Buffer Overflow')			device types during P2P search in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Woice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking CVE ID : CVE-2021-1972	m/company/ product- security/bull etins/august- 2021-bulletin	170921/645
mdm9655					
Out-of- bounds Write	08-Sep-21	10	Possible buffer underflow due to lack of check for negative indices values when processing user provided input in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Voice & Music, Snapdragon Wearables CVE ID : CVE-2021-1916	https://www. qualcomm.co m/company/ product- security/bull etins/august- 2021-bulletin	H-QUA- MDM9- 170921/646
Integer Underflow (Wrap or Wraparoun d)	08-Sep-21	10	Integer underflow can occur when the RTCP length is lesser than than the actual blocks present in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Voice & Music, Snapdragon Wearables	https://www. qualcomm.co m/company/ product- security/bull etins/august- 2021-bulletin	H-QUA- MDM9- 170921/647

0-1

1-2

2-3 3-4

4-5

5-6

6-7

7-8

8-9

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2021-1919		
Integer Underflow (Wrap or Wraparoun d)	08-Sep-21	10	Integer underflow can occur due to improper handling of incoming RTCP packets in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Voice & Music, Snapdragon Wearables CVE ID : CVE-2021-1920	https://www. qualcomm.co m/company/ product- security/bull etins/august- 2021-bulletin	H-QUA- MDM9- 170921/648
msm8108					
Loop with Unreachable Exit Condition ('Infinite Loop')	08-Sep-21	5	Loop with unreachable exit condition may occur due to improper handling of unsupported input in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Voice & Music, Snapdragon Wearables CVE ID : CVE-2021-1914	https://www. qualcomm.co m/company/ product- security/bull etins/august- 2021-bulletin	H-QUA- MSM8- 170921/649
Out-of- bounds Write	08-Sep-21	10	Possible buffer underflow due to lack of check for negative indices values when processing user provided input in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Voice & Music, Snapdragon	https://www. qualcomm.co m/company/ product- security/bull etins/august- 2021-bulletin	H-QUA- MSM8- 170921/650

0-1

1-2

6-7

5-6

7-8

8-9

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Wearables		
			CVE ID : CVE-2021-1916		
Integer Underflow (Wrap or Wraparoun d)	08-Sep-21	10	Integer underflow can occur when the RTCP length is lesser than than the actual blocks present in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Voice & Music, Snapdragon Wearables CVE ID : CVE-2021-1919	https://www. qualcomm.co m/company/ product- security/bull etins/august- 2021-bulletin	H-QUA- MSM8- 170921/651
Integer Underflow (Wrap or Wraparoun d)	08-Sep-21	10	Integer underflow can occur due to improper handling of incoming RTCP packets in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Voice & Music, Snapdragon Wearables CVE ID : CVE-2021-1920	https://www. qualcomm.co m/company/ product- security/bull etins/august- 2021-bulletin	H-QUA- MSM8- 170921/652
msm8208					
Loop with Unreachable Exit Condition ('Infinite Loop')	08-Sep-21	5	Loop with unreachable exit condition may occur due to improper handling of unsupported input in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Voice & Music, Snapdragon	https://www. qualcomm.co m/company/ product- security/bull etins/august- 2021-bulletin	H-QUA- MSM8- 170921/653
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 & CVE ID	Patch	NCIIPC ID
			Wearables		
			CVE ID : CVE-2021-1914		
Out-of- bounds Write	08-Sep-21	10	Possible buffer underflow due to lack of check for negative indices values when processing user provided input in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Voice & Music, Snapdragon Wearables	https://www. qualcomm.co m/company/ product- security/bull etins/august- 2021-bulletin	H-QUA- MSM8- 170921/654
			CVE ID : CVE-2021-1916		
Integer Underflow (Wrap or Wraparoun d)	08-Sep-21	10	Integer underflow can occur when the RTCP length is lesser than than the actual blocks present in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Voice & Music, Snapdragon Wearables CVE ID : CVE-2021-1919	https://www. qualcomm.co m/company/ product- security/bull etins/august- 2021-bulletin	H-QUA- MSM8- 170921/655
Integer Underflow (Wrap or Wraparoun d)	08-Sep-21	10	Integer underflow can occur due to improper handling of incoming RTCP packets in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Voice & Music, Snapdragon Wearables	https://www. qualcomm.co m/company/ product- security/bull etins/august- 2021-bulletin	H-QUA- MSM8- 170921/656
CVSS Scoring Sc	ale 0-1	1-2	2-3 3-4 4-5 5-6	6-7 7-8	8-9 9-10

3-4 4-5 Page 241 of 1474

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2021-1920		
msm8209				I	
Loop with Unreachable Exit Condition ('Infinite Loop')	08-Sep-21	5	Loop with unreachable exit condition may occur due to improper handling of unsupported input in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Voice & Music, Snapdragon Wearables CVE ID : CVE-2021-1914	https://www. qualcomm.co m/company/ product- security/bull etins/august- 2021-bulletin	H-QUA- MSM8- 170921/657
Out-of- bounds Write	08-Sep-21	10	Possible buffer underflow due to lack of check for negative indices values when processing user provided input in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Voice & Music, Snapdragon Wearables CVE ID : CVE-2021-1916	https://www. qualcomm.co m/company/ product- security/bull etins/august- 2021-bulletin	H-QUA- MSM8- 170921/658
Integer Underflow (Wrap or Wraparoun d)	08-Sep-21	10	Integer underflow can occur when the RTCP length is lesser than than the actual blocks present in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Voice & Music, Snapdragon	https://www. qualcomm.co m/company/ product- security/bull etins/august- 2021-bulletin	H-QUA- MSM8- 170921/659

0-1

1-2

6-7

5-6

7-8

8-9

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Wearables		
			CVE ID : CVE-2021-1919		
Integer Underflow (Wrap or Wraparoun d)	08-Sep-21	10	Integer underflow can occur due to improper handling of incoming RTCP packets in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Voice & Music, Snapdragon Wearables CVE ID : CVE-2021-1920	https://www. qualcomm.co m/company/ product- security/bull etins/august- 2021-bulletin	H-QUA- MSM8- 170921/660
msm8608					
Loop with Unreachable Exit Condition ('Infinite Loop')	08-Sep-21	5	Loop with unreachable exit condition may occur due to improper handling of unsupported input in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Voice & Music, Snapdragon Wearables	https://www. qualcomm.co m/company/ product- security/bull etins/august- 2021-bulletin	H-QUA- MSM8- 170921/661
			CVE ID : CVE-2021-1914		
Out-of- bounds Write	08-Sep-21	10	Possible buffer underflow due to lack of check for negative indices values when processing user provided input in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon	https://www. qualcomm.co m/company/ product- security/bull etins/august- 2021-bulletin	H-QUA- MSM8- 170921/662
CVSS Scoring Sc	ale 0-1	1-2	2-3 3-4 4-5 5-6	6-7 7-8	8-9 9-10

Page 243 of 1474

Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
		Voice & Music, Snapdragon Wearables CVE ID : CVE-2021-1916		
08-Sep-21	10	Integer underflow can occur when the RTCP length is lesser than than the actual blocks present in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Voice & Music, Snapdragon Wearables	https://www. qualcomm.co m/company/ product- security/bull etins/august- 2021-bulletin	H-QUA- MSM8- 170921/663
		CVE ID : CVE-2021-1919		
08-Sep-21	10	Integer underflow can occur due to improper handling of incoming RTCP packets in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Voice & Music, Snapdragon Wearables CVE ID : CVE-2021-1920	https://www. qualcomm.co m/company/ product- security/bull etins/august- 2021-bulletin	H-QUA- MSM8- 170921/664
08-Sep-21	2.1	Child process can leak information from parent process due to numeric pids are getting compared and these pid can be reused in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT,	https://www. qualcomm.co m/company/ product- security/bull etins/august- 2021-bulletin	H-QUA- MSM8- 170921/665
	08-Sep-21 08-Sep-21	08-Sep-21 10 08-Sep-21 10 08-Sep-21 10 08-Sep-21 10	Image: Construct of the second seco	Image: constraint of the second sec

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables CVE ID : CVE-2021-1904		
Loop with Unreachable Exit Condition ('Infinite Loop')	08-Sep-21	5	Loop with unreachable exit condition may occur due to improper handling of unsupported input in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Voice & Music, Snapdragon Wearables	https://www. qualcomm.co m/company/ product- security/bull etins/august- 2021-bulletin	H-QUA- MSM8- 170921/666
Out-of- bounds Write	08-Sep-21	10	CVE ID : CVE-2021-1914 Possible buffer underflow due to lack of check for negative indices values when processing user provided input in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Voice & Music, Snapdragon Wearables CVE ID : CVE-2021-1916	https://www. qualcomm.co m/company/ product- security/bull etins/august- 2021-bulletin	H-QUA- MSM8- 170921/667
Integer Underflow (Wrap or Wraparoun d)	08-Sep-21	10	Integer underflow can occur when the RTCP length is lesser than than the actual blocks present in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT,	https://www. qualcomm.co m/company/ product- security/bull etins/august- 2021-bulletin	H-QUA- MSM8- 170921/668

1-2

0-1

5-6

6-7

7-8

8-9

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Snapdragon IoT, Snapdragon Voice & Music, Snapdragon Wearables		
			CVE ID : CVE-2021-1919		
Integer Underflow (Wrap or Wraparoun d)	08-Sep-21	10	Integer underflow can occur due to improper handling of incoming RTCP packets in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Voice & Music, Snapdragon Wearables	https://www. qualcomm.co m/company/ product- security/bull etins/august- 2021-bulletin	H-QUA- MSM8- 170921/669
			CVE ID : CVE-2021-1920		
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	08-Sep-21	10	Possible buffer overflow due to improper validation of device types during P2P search in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Woice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking CVE ID : CVE-2021-1972	https://www. qualcomm.co m/company/ product- security/bull etins/august- 2021-bulletin	H-QUA- MSM8- 170921/670
msm8917					
Exposure of Resource to Wrong Sphere	08-Sep-21	2.1	Child process can leak information from parent process due to numeric pids are getting compared and these pid can be reused in Snapdragon Auto,	https://www. qualcomm.co m/company/ product- security/bull etins/august-	H-QUA- MSM8- 170921/671
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 & CVE ID	Patch	NCIIPC ID
			Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables	2021-bulletin	
			CVE ID : CVE-2021-1904		
Loop with Unreachable Exit Condition ('Infinite Loop')	08-Sep-21	5	Loop with unreachable exit condition may occur due to improper handling of unsupported input in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Voice & Music, Snapdragon Wearables CVE ID : CVE-2021-1914	https://www. qualcomm.co m/company/ product- security/bull etins/august- 2021-bulletin	H-QUA- MSM8- 170921/672
Out-of- bounds Write	08-Sep-21	10	Possible buffer underflow due to lack of check for negative indices values when processing user provided input in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Voice & Music, Snapdragon Wearables CVE ID : CVE-2021-1916	https://www. qualcomm.co m/company/ product- security/bull etins/august- 2021-bulletin	H-QUA- MSM8- 170921/673
Integer Underflow (Wrap or Wraparoun	08-Sep-21	10	Integer underflow can occur when the RTCP length is lesser than than the actual blocks present in Snapdragon	https://www. qualcomm.co m/company/ product-	H-QUA- MSM8- 170921/674

CVSS Scoring Scale	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10
Page 247 of 1474										

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
d)			Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Voice & Music, Snapdragon Wearables	security/bull etins/august- 2021-bulletin	
			CVE ID : CVE-2021-1919		
Integer Underflow (Wrap or Wraparoun d)	08-Sep-21	10	Integer underflow can occur due to improper handling of incoming RTCP packets in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Voice & Music, Snapdragon Wearables	https://www. qualcomm.co m/company/ product- security/bull etins/august- 2021-bulletin	H-QUA- MSM8- 170921/675
			CVE ID : CVE-2021-1920		
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	08-Sep-21	10	Possible buffer overflow due to improper validation of device types during P2P search in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Woice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking CVE ID : CVE-2021-1972	https://www. qualcomm.co m/company/ product- security/bull etins/august- 2021-bulletin	H-QUA- MSM8- 170921/676
msm8920					
Loop with Unreachable	08-Sep-21	5	Loop with unreachable exit condition may occur due to	https://www. qualcomm.co	H-QUA- MSM8-
CVSS Scoring Sc	ale 0-1	1-2	2-3 3-4 4-5 5-6 Page 248 of 1474	6-7 7-8	8-9 9-10

Page 248 of 1474

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Exit Condition ('Infinite Loop')			improper handling of unsupported input in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Voice & Music, Snapdragon Wearables CVE ID : CVE-2021-1914	m/company/ product- security/bull etins/august- 2021-bulletin	170921/677
Out-of- bounds Write	08-Sep-21	10	Possible buffer underflow due to lack of check for negative indices values when processing user provided input in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Voice & Music, Snapdragon Wearables CVE ID : CVE-2021-1916	https://www. qualcomm.co m/company/ product- security/bull etins/august- 2021-bulletin	H-QUA- MSM8- 170921/678
Integer Underflow (Wrap or Wraparoun d)	08-Sep-21	10	Integer underflow can occur when the RTCP length is lesser than than the actual blocks present in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Voice & Music, Snapdragon Wearables CVE ID : CVE-2021-1919	https://www. qualcomm.co m/company/ product- security/bull etins/august- 2021-bulletin	H-QUA- MSM8- 170921/679
Integer Underflow	08-Sep-21	10	Integer underflow can occur due to improper handling of	https://www. qualcomm.co	H-QUA- MSM8-

CVSS Scoring Scale	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10
Page 249 of 1474										

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
(Wrap or Wraparoun d)			incoming RTCP packets in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Voice & Music, Snapdragon Wearables CVE ID : CVE-2021-1920	m/company/ product- security/bull etins/august- 2021-bulletin	170921/680
msm8937					
Loop with Unreachable Exit Condition ('Infinite Loop')	08-Sep-21	5	Loop with unreachable exit condition may occur due to improper handling of unsupported input in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Voice & Music, Snapdragon Wearables CVE ID : CVE-2021-1914	https://www. qualcomm.co m/company/ product- security/bull etins/august- 2021-bulletin	H-QUA- MSM8- 170921/681
Out-of- bounds Write	08-Sep-21	10	Possible buffer underflow due to lack of check for negative indices values when processing user provided input in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Voice & Music, Snapdragon Wearables CVE ID : CVE-2021-1916	https://www. qualcomm.co m/company/ product- security/bull etins/august- 2021-bulletin	H-QUA- MSM8- 170921/682
Integer	08-Sep-21	10	Integer underflow can occur	https://www.	H-QUA-
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 & CVE ID	Patch	NCIIPC ID
Underflow (Wrap or Wraparoun d)			when the RTCP length is lesser than than the actual blocks present in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Voice & Music, Snapdragon Wearables CVE ID : CVE-2021-1919	qualcomm.co m/company/ product- security/bull etins/august- 2021-bulletin	MSM8- 170921/683
Integer Underflow (Wrap or Wraparoun d)	08-Sep-21	10	Integer underflow can occur due to improper handling of incoming RTCP packets in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Voice & Music, Snapdragon Wearables CVE ID : CVE-2021-1920	https://www. qualcomm.co m/company/ product- security/bull etins/august- 2021-bulletin	H-QUA- MSM8- 170921/684
msm8940					
Loop with Unreachable Exit Condition ('Infinite Loop')		Loop with unreachable exit condition may occur due to improper handling of unsupported input in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Voice & Music, Snapdragon Wearables CVE ID : CVE-2021-1914	https://www. qualcomm.co m/company/ product- security/bull etins/august- 2021-bulletin	H-QUA- MSM8- 170921/685	
Out-of-	08-Sep-21	10	Possible buffer underflow	https://www.	H-QUA-
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 & CVE ID	Patch	NCIIPC ID
bounds Write			due to lack of check for negative indices values when processing user provided input in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Voice & Music, Snapdragon Wearables CVE ID : CVE-2021-1916	qualcomm.co m/company/ product- security/bull etins/august- 2021-bulletin	MSM8- 170921/686
Integer Underflow (Wrap or Wraparoun d)	08-Sep-21	10	Integer underflow can occur when the RTCP length is lesser than than the actual blocks present in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Voice & Music, Snapdragon Wearables CVE ID : CVE-2021-1919	https://www. qualcomm.co m/company/ product- security/bull etins/august- 2021-bulletin	H-QUA- MSM8- 170921/687
Integer Underflow (Wrap or Wraparoun d)	08-Sep-21	10	Integer underflow can occur due to improper handling of incoming RTCP packets in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Voice & Music, Snapdragon Wearables CVE ID : CVE-2021-1920	https://www. qualcomm.co m/company/ product- security/bull etins/august- 2021-bulletin	H-QUA- MSM8- 170921/688
msm8953					
	08-Sep-21	2.1	Child process can leak	https://www.	H-QUA-

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Resource to Wrong Sphere			information from parent process due to numeric pids are getting compared and these pid can be reused in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wearables CVE ID : CVE-2021-1904	qualcomm.co m/company/ product- security/bull etins/august- 2021-bulletin	MSM8- 170921/689
Loop with Unreachable Exit Condition ('Infinite Loop')	08-Sep-21	5	Loop with unreachable exit condition may occur due to improper handling of unsupported input in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Voice & Music, Snapdragon Wearables CVE ID : CVE-2021-1914	https://www. qualcomm.co m/company/ product- security/bull etins/august- 2021-bulletin	H-QUA- MSM8- 170921/690
Out-of- bounds Write	08-Sep-21	10	Possible buffer underflow due to lack of check for negative indices values when processing user provided input in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Voice & Music, Snapdragon Wearables	https://www. qualcomm.co m/company/ product- security/bull etins/august- 2021-bulletin	H-QUA- MSM8- 170921/691

CVSS Scoring Scale	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10
Dage 252 of 1474										

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2021-1916		
Integer Underflow (Wrap or Wraparoun d)	08-Sep-21	10	Integer underflow can occur when the RTCP length is lesser than than the actual blocks present in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Voice & Music, Snapdragon Wearables CVE ID : CVE-2021-1919	https://www. qualcomm.co m/company/ product- security/bull etins/august- 2021-bulletin	H-QUA- MSM8- 170921/692
Integer Underflow (Wrap or Wraparoun d)	08-Sep-21	10	Integer underflow can occur due to improper handling of incoming RTCP packets in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Voice & Music, Snapdragon Wearables CVE ID : CVE-2021-1920	https://www. qualcomm.co m/company/ product- security/bull etins/august- 2021-bulletin	H-QUA- MSM8- 170921/693
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	08-Sep-21	10	Possible buffer overflow due to improper validation of device types during P2P search in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Woice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and	https://www. qualcomm.co m/company/ product- security/bull etins/august- 2021-bulletin	H-QUA- MSM8- 170921/694

CVSS Scoring Scale	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10
			Р	age 254 c	of 1474					

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Networking		
			CVE ID : CVE-2021-1972		
msm8976					
Loop with Unreachable Exit Condition ('Infinite Loop')	08-Sep-21	5	Loop with unreachable exit condition may occur due to improper handling of unsupported input in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Voice & Music, Snapdragon Wearables CVE ID : CVE-2021-1914	https://www. qualcomm.co m/company/ product- security/bull etins/august- 2021-bulletin	H-QUA- MSM8- 170921/695
Out-of- bounds Write	08-Sep-21	10	Possible buffer underflow due to lack of check for negative indices values when processing user provided input in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Voice & Music, Snapdragon Wearables CVE ID : CVE-2021-1916	https://www. qualcomm.co m/company/ product- security/bull etins/august- 2021-bulletin	H-QUA- MSM8- 170921/696
Integer Underflow (Wrap or Wraparoun d)	08-Sep-21	10	Integer underflow can occur when the RTCP length is lesser than than the actual blocks present in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon	https://www. qualcomm.co m/company/ product- security/bull etins/august- 2021-bulletin	H-QUA- MSM8- 170921/697
CVSS Scoring Sc	ale 0-1	1-2	2-3 3-4 4-5 5-6	6-7 7-8	8-9 9-10

Page 255 of 1474

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Voice & Music, Snapdragon Wearables CVE ID : CVE-2021-1919		
Integer Underflow (Wrap or Wraparoun d)	08-Sep-21	10	Integer underflow can occur due to improper handling of incoming RTCP packets in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Voice & Music, Snapdragon Wearables CVE ID : CVE-2021-1920	https://www. qualcomm.co m/company/ product- security/bull etins/august- 2021-bulletin	H-QUA- MSM8- 170921/698
msm8976sg					
Loop with Unreachable Exit Condition ('Infinite Loop')	08-Sep-21	5	Loop with unreachable exit condition may occur due to improper handling of unsupported input in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Voice & Music, Snapdragon Wearables CVE ID : CVE-2021-1914	https://www. qualcomm.co m/company/ product- security/bull etins/august- 2021-bulletin	H-QUA- MSM8- 170921/699
Out-of- bounds Write	08-Sep-21	10	Possible buffer underflow due to lack of check for negative indices values when processing user provided input in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT,	https://www. qualcomm.co m/company/ product- security/bull etins/august- 2021-bulletin	H-QUA- MSM8- 170921/700
CVSS Scoring Sc	ale 0-1	1-2	2-3 3-4 4-5 5-6	6-7 7-8	8-9 9-10

Page 256 of 1474

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Snapdragon IoT, Snapdragon Voice & Music, Snapdragon Wearables		
			CVE ID : CVE-2021-1916		
Integer Underflow (Wrap or Wraparoun d)	08-Sep-21	10	Integer underflow can occur when the RTCP length is lesser than than the actual blocks present in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Voice & Music, Snapdragon Wearables	https://www. qualcomm.co m/company/ product- security/bull etins/august- 2021-bulletin	H-QUA- MSM8- 170921/701
			CVE ID : CVE-2021-1919		
Integer Underflow (Wrap or Wraparoun d)	08-Sep-21	10	Integer underflow can occur due to improper handling of incoming RTCP packets in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Voice & Music, Snapdragon Wearables CVE ID : CVE-2021-1920	https://www. qualcomm.co m/company/ product- security/bull etins/august- 2021-bulletin	H-QUA- MSM8- 170921/702
msm8996au					
Exposure of Resource to Wrong Sphere	08-Sep-21	2.1	Child process can leak information from parent process due to numeric pids are getting compared and these pid can be reused in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT,	https://www. qualcomm.co m/company/ product- security/bull etins/august- 2021-bulletin	H-QUA- MSM8- 170921/703
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 & CVE ID	Patch	NCIIPC ID
			Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables		
			CVE ID : CVE-2021-1904		
Loop with Unreachable Exit Condition ('Infinite Loop')	08-Sep-21	5	Loop with unreachable exit condition may occur due to improper handling of unsupported input in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Voice & Music, Snapdragon Wearables	https://www. qualcomm.co m/company/ product- security/bull etins/august- 2021-bulletin	H-QUA- MSM8- 170921/704
			CVE ID : CVE-2021-1914		
Out-of- bounds Write	08-Sep-21	10	Possible buffer underflow due to lack of check for negative indices values when processing user provided input in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Voice & Music, Snapdragon Wearables CVE ID : CVE-2021-1916	https://www. qualcomm.co m/company/ product- security/bull etins/august- 2021-bulletin	H-QUA- MSM8- 170921/705
Integer Underflow (Wrap or Wraparoun d)	08-Sep-21	10	Integer underflow can occur when the RTCP length is lesser than than the actual blocks present in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT,	https://www. qualcomm.co m/company/ product- security/bull etins/august- 2021-bulletin	H-QUA- MSM8- 170921/706
CVSS Scoring Sco	ale 0-1	1-2	2-3 3-4 4-5 5-6 Page 258 of 1474	6-7 7-8	8-9 9-10

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Voice & Music, Snapdragon Wearables CVE ID : CVE-2021-1919		
			Integer underflow can occur due to improper handling of		
Integer Underflow (Wrap or Wraparoun d)	08-Sep-21	10	incoming RTCP packets in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Voice & Music, Snapdragon Wearables	https://www. qualcomm.co m/company/ product- security/bull etins/august- 2021-bulletin	H-QUA- MSM8- 170921/707
			CVE ID : CVE-2021-1920		
Exposure of Resource to Wrong Sphere	08-Sep-21	2.1	Lack of strict validation of bootmode can lead to information disclosure in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wearables	https://www. qualcomm.co m/company/ product- security/bull etins/august- 2021-bulletin	H-QUA- MSM8- 170921/708
			CVE ID : CVE-2021-1929		
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	08-Sep-21	10	Possible buffer overflow due to improper validation of device types during P2P search in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music,	https://www. qualcomm.co m/company/ product- security/bull etins/august- 2021-bulletin	H-QUA- MSM8- 170921/709

0-1

1-2

7-8

5-6

6-7

8-9

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking		
			CVE ID : CVE-2021-1972		
pmp8074	I			I	L
Out-of- bounds Read	08-Sep-21	3.6	Buffer over read could occur due to incorrect check of buffer size while flashing emmc devices in Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking CVE ID : CVE-2021-1928	https://www. qualcomm.co m/company/ product- security/bull etins/august- 2021-bulletin	H-QUA-PMP8- 170921/710
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	08-Sep-21	10	Possible buffer overflow due to improper validation of device types during P2P search in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Woice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking CVE ID : CVE-2021-1972	https://www. qualcomm.co m/company/ product- security/bull etins/august- 2021-bulletin	H-QUA-PMP8- 170921/711
qca1990					
Out-of- bounds	08-Sep-21	10	Possible buffer underflow due to lack of check for negative indices values when	https://www. qualcomm.co m/company/	H-QUA-QCA1- 170921/712
CVSS Scoring Sc	ale 0-1	1-2	2-3 3-4 4-5 5-6 Page 260 of 1474	6-7 7-8	8-9 <mark>9-10</mark>

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Write			processing user provided input in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Voice & Music, Snapdragon Wearables CVE ID : CVE-2021-1916	product- security/bull etins/august- 2021-bulletin	
Integer Underflow (Wrap or Wraparoun d)	08-Sep-21	10	Integer underflow can occur due to improper handling of incoming RTCP packets in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Voice & Music, Snapdragon Wearables CVE ID : CVE-2021-1920	https://www. qualcomm.co m/company/ product- security/bull etins/august- 2021-bulletin	H-QUA-QCA1- 170921/713
qca4004					I
Loop with Unreachable Exit Condition ('Infinite Loop')	08-Sep-21	5	Loop with unreachable exit condition may occur due to improper handling of unsupported input in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Voice & Music, Snapdragon Wearables CVE ID : CVE-2021-1914	https://www. qualcomm.co m/company/ product- security/bull etins/august- 2021-bulletin	H-QUA-QCA4- 170921/714
Out-of- bounds	08-Sep-21	10	Possible buffer underflow due to lack of check for	https://www. qualcomm.co	H-QUA-QCA4- 170921/715

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Write			negative indices values when processing user provided input in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Voice & Music, Snapdragon Wearables CVE ID : CVE-2021-1916	m/company/ product- security/bull etins/august- 2021-bulletin	
Integer Underflow (Wrap or Wraparoun d)	08-Sep-21	10	Integer underflow can occur due to improper handling of incoming RTCP packets in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Voice & Music, Snapdragon Wearables CVE ID : CVE-2021-1920	https://www. qualcomm.co m/company/ product- security/bull etins/august- 2021-bulletin	H-QUA-QCA4- 170921/716
qca4020					L
Exposure of Resource to Wrong Sphere	08-Sep-21	2.1	Child process can leak information from parent process due to numeric pids are getting compared and these pid can be reused in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wearables CVE ID : CVE-2021-1904	https://www. qualcomm.co m/company/ product- security/bull etins/august- 2021-bulletin	H-QUA-QCA4- 170921/717
CVSS Scoring Sca	ale 0-1	1-2	2-3 3-4 4-5 5-6	6-7 7-8	8-9 9-10

3-4 4-5 Page 262 of 1474

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	08-Sep-21	10	Possible buffer overflow due to improper validation of device types during P2P search in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Woice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking CVE ID : CVE-2021-1972	https://www. qualcomm.co m/company/ product- security/bull etins/august- 2021-bulletin	H-QUA-QCA4- 170921/718
qca4024	L			l	
Out-of- bounds Read	08-Sep-21	3.6	Buffer over read could occur due to incorrect check of buffer size while flashing emmc devices in Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking CVE ID : CVE-2021-1928	https://www. qualcomm.co m/company/ product- security/bull etins/august- 2021-bulletin	H-QUA-QCA4- 170921/719
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	08-Sep-21	10	Possible buffer overflow due to improper validation of device types during P2P search in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music,	https://www. qualcomm.co m/company/ product- security/bull etins/august- 2021-bulletin	H-QUA-QCA4- 170921/720

Wrong Sphere08-Sep-212.1Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Mobile, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearablesproduct- security/bull etins/august- 2021-bulletin170921/721Out-of- bounds08-Sep-2108-Sep-21Possible buffer underflow due to lack of check for negative indices values when processing user provided input in Snapdragon Connectivity, Snapdragon Connectivity, Snapdragon Connectivity, Snapdragon Connectivity, Snapdragon Connectivity, Snapdragon Iot, Snapdragon Voice & Music, Snapdrago	Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
qca6174Exposure of Resource to Wrong Sphere08-Sep-21Child process can leak information from parent process due to numeric pids are getting compared and these pid can be reused in Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Mobile, Snapdragon Mobile, Snapdragon Mobile, Snapdragon Mobile, Snapdragon Mobile, Snapdragon Mobile, Snapdragon Mobile, Snapdragon Consumer IOT, Snapdragon Mobile, Snapdragon Mobile, Snapdragon Consumer IOT, Snapdragon Mobile, Snapdragon Mobile, Snapdragon Consumer IOT, Snapdragon Mobile, Snapdragon Consumer IOT, Snapdragon Consumer IOT, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Industrial IOT, Snapdragon Industrial IOT, Snapdragon Industrial IOT, Snapdragon Industrial IOT, Snapdragon Iot, Snapdragon Voice & Music, Snapdrago				Snapdragon Wired Infrastructure and		
Exposure of Resource to Wrong Sphere08-Sep-21Child process can leak 				CVE ID : CVE-2021-1972		
Exposure of Resource to Wrong Sphere08-Sep-212.1information from parent process due to numeric pids are getting compared and these pid can be reused in Snapdragon Conpute, Snapdragon Consumer 10T, Snapdragon Mubile, Snapdragon Mobile, Snapdragon Noice & Music, Snapdragon Wearableshttps://www. qualcomn.co m/company/ product- security/bull etins/august- 2021-bulletinH-QUA-QCA6- 170921/721Out-of- bounds Write08-Sep-2108-Sep-21Possible buffer underflow due to lack of check for negative indices values when processing user provided input in Snapdragon Consumer 10T, Snapdragon Compute, Snapdragon Consumer 10T, Snapdragon Industrial 10T, Snapdragon Industria	qca6174				I	L
Out-of- bounds08-Sep-2110due to lack of check for negative indices values when processing user provided input in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Industrial IOT, Snapdragon Industrial IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon 2021-bulletinH-QUA-QCA6- 170921/722Integer Underflow (Wrap or Wraparoun08-Sep-2110Integer underflow can occur incoming RTCP packets in Snapdragon Auto,https://www. qualcomm.co m/company/ product- security/bull etins/august- 2021-bulletinH-QUA-QCA6- 170921/722	Resource to Wrong	08-Sep-21	2.1	information from parent process due to numeric pids are getting compared and these pid can be reused in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wearables	qualcomm.co m/company/ product- security/bull etins/august-	H-QUA-QCA6- 170921/721
Underflow (Wrap or Wraparoun08-Sep-2110Integer underflow improper handling of incoming RTCP packets in Snapdragon Auto,qualcomm.co m/company/ product-H-QUA-QCA6- 170921/723	bounds	08-Sep-21	10	due to lack of check for negative indices values when processing user provided input in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Voice & Music, Snapdragon Wearables	qualcomm.co m/company/ product- security/bull etins/august-	H-QUA-QCA6- 170921/722
	Underflow (Wrap or Wraparoun	08-Sep-21	10	due to improper handling of incoming RTCP packets in	qualcomm.co m/company/	H-QUA-QCA6- 170921/723

Page 264 of 1474

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Voice & Music, Snapdragon Wearables	etins/august- 2021-bulletin	
			CVE ID : CVE-2021-1920		
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	08-Sep-21	10	Possible buffer overflow due to improper validation of device types during P2P search in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Woice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking CVE ID : CVE-2021-1972	https://www. qualcomm.co m/company/ product- security/bull etins/august- 2021-bulletin	H-QUA-QCA6- 170921/724
qca6174a					
Exposure of Resource to Wrong Sphere	08-Sep-21	2.1	Child process can leak information from parent process due to numeric pids are getting compared and these pid can be reused in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wearables CVE ID : CVE-2021-1904	https://www. qualcomm.co m/company/ product- security/bull etins/august- 2021-bulletin	H-QUA-QCA6- 170921/725
Loop with	08-Sep-21	5	Loop with unreachable exit	https://www.	H-QUA-QCA6-

		condition may occur due to improper handling of unsupported input in Snapdragon Auto,	qualcomm.co m/company/ product-	170921/726
		Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Voice & Music, Snapdragon Wearables	security/bull etins/august- 2021-bulletin	
		CVE ID : CVE-2021-1914		
3-Sep-21	10	Possible buffer underflow due to lack of check for negative indices values when processing user provided input in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Voice & Music, Snapdragon Wearables	https://www. qualcomm.co m/company/ product- security/bull etins/august- 2021-bulletin	H-QUA-QCA6- 170921/727
3-Sep-21	10	when the RTCP length is lesser than than the actual blocks present in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Voice & Music, Snapdragon Wearables	https://www. qualcomm.co m/company/ product- security/bull etins/august- 2021-bulletin	H-QUA-QCA6- 170921/728
3-Sep-21	10	Integer underflow can occur	https://www.	H-QUA-QCA6-
3-	- Sep-21	·Sep-21 10	Sep-2110Wearables•Sep-2110Possible buffer underflow due to lack of check for negative indices values when processing user provided input in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Voice & Music, Snapdragon Wearables•Sep-2110Integer underflow can occur when the RTCP length is lesser than than the actual blocks present in Snapdragon Compute, Snapdragon Connectivity, Snapdragon Connectivity, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Connectivity, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Industrial IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon IoT, Snapdragon Voice & Music, Snapdragon Voice & Music, Snapdragon Voice & Music, Snapdragon IoT, Snapdragon IoT, Snapdragon IoT, Snapdragon IoT, Snapdragon IoT, Snapdragon Voice & Music, Snapdragon Voice & Musi	WearablesCVE ID : CVE-2021-1914Possible buffer underflow due to lack of check for negative indices values when processing user provided input in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Voice & Music, Snapdragon Wearableshttps://www. qualcomm.co m/company/ product- security/bull etins/august- 2021-bulletin-Sep-2110Integer underflow can occur when the RTCP length is lesser than than the actual blocks present in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer IOT, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Compute, Snapdragon Industrial IOT, Snapdragon Consumer IOT, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Voice & Music, Snapdragonhttps://wwwSep-2110

Page 266 of 1474

Underflow (Wrap or Wraparoun d) Improper Restriction of			due to improper handling of incoming RTCP packets in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Voice & Music, Snapdragon Wearables CVE ID : CVE-2021-1920	qualcomm.co m/company/ product- security/bull etins/august- 2021-bulletin	170921/729
Restriction					
Operations	08-Sep-21	3.6	Possible out of bounds read due to incorrect validation of incoming buffer length in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile CVE ID : CVE-2021-1930	https://www. qualcomm.co m/company/ product- security/bull etins/august- 2021-bulletin	H-QUA-QCA6- 170921/730
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	08-Sep-21	10	Possible buffer overflow due to improper validation of device types during P2P search in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Woice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking CVE ID : CVE-2021-1972	https://www. qualcomm.co m/company/ product- security/bull etins/august- 2021-bulletin	H-QUA-QCA6- 170921/731
qca6310					
Exposure of (08-Sep-21	2.1	Child process can leak	https://www.	H-QUA-QCA6-

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Resource to Wrong Sphere			information from parent process due to numeric pids are getting compared and these pid can be reused in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wearables CVE ID : CVE-2021-1904	qualcomm.co m/company/ product- security/bull etins/august- 2021-bulletin	170921/732
Loop with Unreachable Exit Condition ('Infinite Loop')	08-Sep-21	5	Loop with unreachable exit condition may occur due to improper handling of unsupported input in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Voice & Music, Snapdragon Wearables CVE ID : CVE-2021-1914	https://www. qualcomm.co m/company/ product- security/bull etins/august- 2021-bulletin	H-QUA-QCA6- 170921/733
Out-of- bounds Write	08-Sep-21	10	Possible buffer underflow due to lack of check for negative indices values when processing user provided input in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Voice & Music, Snapdragon Wearables	https://www. qualcomm.co m/company/ product- security/bull etins/august- 2021-bulletin	H-QUA-QCA6- 170921/734

CVSS Scoring Scale	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10
Dago 268 of 1474										

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2021-1916		
Integer Underflow (Wrap or Wraparoun d)	08-Sep-21	10	Integer underflow can occur when the RTCP length is lesser than than the actual blocks present in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Voice & Music, Snapdragon Wearables CVE ID : CVE-2021-1919	https://www. qualcomm.co m/company/ product- security/bull etins/august- 2021-bulletin	H-QUA-QCA6- 170921/735
Integer Underflow (Wrap or Wraparoun d)	08-Sep-21	10	Integer underflow can occur due to improper handling of incoming RTCP packets in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Voice & Music, Snapdragon Wearables CVE ID : CVE-2021-1920	https://www. qualcomm.co m/company/ product- security/bull etins/august- 2021-bulletin	H-QUA-QCA6- 170921/736
Out-of- bounds Read	08-Sep-21	3.6	Buffer over read could occur due to incorrect check of buffer size while flashing emmc devices in Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking CVE ID : CVE-2021-1928	https://www. qualcomm.co m/company/ product- security/bull etins/august- 2021-bulletin	H-QUA-QCA6- 170921/737

 3-4
 4-5
 5-6

 Page 269 of 1474

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	08-Sep-21	10	Possible buffer overflow due to improper validation of device types during P2P search in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Woice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking CVE ID : CVE-2021-1972	https://www. qualcomm.co m/company/ product- security/bull etins/august- 2021-bulletin	H-QUA-QCA6- 170921/738
qca6320	L			I	
Exposure of Resource to Wrong Sphere	08-Sep-21	2.1	Child process can leak information from parent process due to numeric pids are getting compared and these pid can be reused in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables CVE ID : CVE-2021-1904	https://www. qualcomm.co m/company/ product- security/bull etins/august- 2021-bulletin	H-QUA-QCA6- 170921/739
Loop with Unreachable Exit Condition ('Infinite Loop')	08-Sep-21	5	Loop with unreachable exit condition may occur due to improper handling of unsupported input in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT,	https://www. qualcomm.co m/company/ product- security/bull etins/august- 2021-bulletin	H-QUA-QCA6- 170921/740

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Snapdragon IoT, Snapdragon Voice & Music, Snapdragon Wearables		
			CVE ID : CVE-2021-1914		
Out-of- bounds Write	08-Sep-21	10	Possible buffer underflow due to lack of check for negative indices values when processing user provided input in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Voice & Music, Snapdragon Wearables	https://www. qualcomm.co m/company/ product- security/bull etins/august- 2021-bulletin	H-QUA-QCA6- 170921/741
			CVE ID : CVE-2021-1916		
Integer Underflow (Wrap or Wraparoun d)	08-Sep-21	10	Integer underflow can occur when the RTCP length is lesser than than the actual blocks present in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Voice & Music, Snapdragon Wearables	https://www. qualcomm.co m/company/ product- security/bull etins/august- 2021-bulletin	H-QUA-QCA6- 170921/742
			CVE ID : CVE-2021-1919		
Integer Underflow (Wrap or Wraparoun d)	08-Sep-21	10	Integer underflow can occur due to improper handling of incoming RTCP packets in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon	https://www. qualcomm.co m/company/ product- security/bull etins/august- 2021-bulletin	H-QUA-QCA6- 170921/743

1-2

0-1

6-7

5-6

7-8

8-9

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID	
			Voice & Music, Snapdragon Wearables			
			CVE ID : CVE-2021-1920			
Out-of- bounds Read	08-Sep-21	3.6	Buffer over read could occur due to incorrect check of buffer size while flashing emmc devices in Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking	https://www. qualcomm.co m/company/ product- security/bull etins/august- 2021-bulletin	H-QUA-QCA6- 170921/744	
			CVE ID : CVE-2021-1928			
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	08-Sep-21	10	Possible buffer overflow due to improper validation of device types during P2P search in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Woice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking CVE ID : CVE-2021-1972	https://www. qualcomm.co m/company/ product- security/bull etins/august- 2021-bulletin	H-QUA-QCA6- 170921/745	
qca6335						
Exposure of Resource to Wrong Sphere	08-Sep-21	2.1	Child process can leak information from parent process due to numeric pids are getting compared and these pid can be reused in Snapdragon Auto,	https://www. qualcomm.co m/company/ product- security/bull etins/august-	H-QUA-QCA6- 170921/746	
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 & CVE ID	Patch	NCIIPC ID
			Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables	2021-bulletin	
			CVE ID : CVE-2021-1904		
Loop with Unreachable Exit Condition ('Infinite Loop')	08-Sep-21	5	Loop with unreachable exit condition may occur due to improper handling of unsupported input in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Voice & Music, Snapdragon Wearables CVE ID : CVE-2021-1914	https://www. qualcomm.co m/company/ product- security/bull etins/august- 2021-bulletin	H-QUA-QCA6- 170921/747
Out-of- bounds Write	08-Sep-21	10	Possible buffer underflow due to lack of check for negative indices values when processing user provided input in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Voice & Music, Snapdragon Wearables CVE ID : CVE-2021-1916	https://www. qualcomm.co m/company/ product- security/bull etins/august- 2021-bulletin	H-QUA-QCA6- 170921/748
Integer Underflow (Wrap or Wraparoun	08-Sep-21	10	Integer underflow can occur when the RTCP length is lesser than than the actual blocks present in Snapdragon	https://www. qualcomm.co m/company/ product-	H-QUA-QCA6- 170921/749

CVSS Scoring Scale	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10
Page 273 of 1/17/										

Page 273 of 1474

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
d)			Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Voice & Music, Snapdragon Wearables	security/bull etins/august- 2021-bulletin	
			CVE ID : CVE-2021-1919		
Integer Underflow (Wrap or Wraparoun d)	08-Sep-21	10	Integer underflow can occur due to improper handling of incoming RTCP packets in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Voice & Music, Snapdragon Wearables CVE ID : CVE-2021-1920	https://www. qualcomm.co m/company/ product- security/bull etins/august- 2021-bulletin	H-QUA-QCA6- 170921/750
Out-of- bounds Read	08-Sep-21	3.6	Buffer over read could occur due to incorrect check of buffer size while flashing emmc devices in Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking CVE ID : CVE-2021-1928	https://www. qualcomm.co m/company/ product- security/bull etins/august- 2021-bulletin	H-QUA-QCA6- 170921/751
Buffer Copy without Checking Size of Input ('Classic	08-Sep-21	10	Possible buffer overflow due to improper validation of device types during P2P search in Snapdragon Auto, Snapdragon Compute,	https://www. qualcomm.co m/company/ product- security/bull	H-QUA-QCA6- 170921/752

0-1

1-2

6-7

5-6

7-8

8-9

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Buffer Overflow')			Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking CVE ID : CVE-2021-1972	etins/august- 2021-bulletin	
qca6390				1	
Exposure of Resource to Wrong Sphere	08-Sep-21	2.1	Child process can leak information from parent process due to numeric pids are getting compared and these pid can be reused in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wearables CVE ID : CVE-2021-1904	https://www. qualcomm.co m/company/ product- security/bull etins/august- 2021-bulletin	H-QUA-QCA6- 170921/753
Loop with Unreachable Exit Condition ('Infinite Loop')	08-Sep-21	5	Loop with unreachable exit condition may occur due to improper handling of unsupported input in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Voice & Music, Snapdragon Wearables CVE ID : CVE-2021-1914	https://www. qualcomm.co m/company/ product- security/bull etins/august- 2021-bulletin	H-QUA-QCA6- 170921/754
CVSS Scoring Sc	ale 0-1	1-2	2-3 3-4 4-5 5-6	6-7 7-8	8-9 9-10

 3-4
 4-5
 5-6
 6-7

 Page 275 of 1474

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Out-of- bounds Write	08-Sep-21	10	Possible buffer underflow due to lack of check for negative indices values when processing user provided input in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Voice & Music, Snapdragon Wearables CVE ID : CVE-2021-1916	https://www. qualcomm.co m/company/ product- security/bull etins/august- 2021-bulletin	H-QUA-QCA6- 170921/755
Integer Underflow (Wrap or Wraparoun d)	08-Sep-21	10	Integer underflow can occur when the RTCP length is lesser than than the actual blocks present in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Voice & Music, Snapdragon Wearables CVE ID : CVE-2021-1919	https://www. qualcomm.co m/company/ product- security/bull etins/august- 2021-bulletin	H-QUA-QCA6- 170921/756
Integer Underflow (Wrap or Wraparoun d)	08-Sep-21	10	Integer underflow can occur due to improper handling of incoming RTCP packets in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Voice & Music, Snapdragon Wearables	https://www. qualcomm.co m/company/ product- security/bull etins/august- 2021-bulletin	H-QUA-QCA6- 170921/757
Incorrect	08-Sep-21	4.6	CVE ID : CVE-2021-1920 Incorrect pointer argument	https://www.	H-QUA-QCA6-
meonreet	1		meorreet pointer argument	neep5.//	

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Type Conversion or Cast			passed to trusted application TA could result in un- intended memory operations in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Industrial IOT CVE ID : CVE-2021-1923	qualcomm.co m/company/ product- security/bull etins/august- 2021-bulletin	170921/758
Exposure of Resource to Wrong Sphere	08-Sep-21	2.1	Lack of strict validation of bootmode can lead to information disclosure in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wearables CVE ID : CVE-2021-1929	https://www. qualcomm.co m/company/ product- security/bull etins/august- 2021-bulletin	H-QUA-QCA6- 170921/759
Improper Restriction of Operations within the Bounds of a Memory Buffer	08-Sep-21	3.6	Possible out of bounds read due to incorrect validation of incoming buffer length in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile CVE ID : CVE-2021-1930	https://www. qualcomm.co m/company/ product- security/bull etins/august- 2021-bulletin	H-QUA-QCA6- 170921/760
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	08-Sep-21	10	Possible buffer overflow due to improper validation of device types during P2P search in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile,	https://www. qualcomm.co m/company/ product- security/bull etins/august- 2021-bulletin	H-QUA-QCA6- 170921/761

0-1

1-2

4-5

5-6

6-7

7-8

8-9

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking		
			CVE ID : CVE-2021-1972		
qca6391					
Exposure of Resource to Wrong Sphere	08-Sep-21	2.1	Child process can leak information from parent process due to numeric pids are getting compared and these pid can be reused in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wearables CVE ID : CVE-2021-1904	https://www. qualcomm.co m/company/ product- security/bull etins/august- 2021-bulletin	H-QUA-QCA6- 170921/762
Loop with Unreachable Exit Condition ('Infinite Loop')	08-Sep-21	5	Loop with unreachable exit condition may occur due to improper handling of unsupported input in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Voice & Music, Snapdragon Wearables CVE ID : CVE-2021-1914	https://www. qualcomm.co m/company/ product- security/bull etins/august- 2021-bulletin	H-QUA-QCA6- 170921/763
Out-of- bounds Write	08-Sep-21	10	Possible buffer underflow due to lack of check for negative indices values when processing user provided	https://www. qualcomm.co m/company/ product-	H-QUA-QCA6- 170921/764
CVSS Scoring Sc	ale 0-1	1-2	2-3 3-4 4-5 5-6	6-7 7-8	8-9 9-10

Page 278 of 1474

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			input in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Voice & Music, Snapdragon Wearables	security/bull etins/august- 2021-bulletin	
			CVE ID : CVE-2021-1916		
Integer Underflow (Wrap or Wraparoun d)	08-Sep-21	10	Integer underflow can occur when the RTCP length is lesser than than the actual blocks present in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Voice & Music, Snapdragon Wearables CVE ID : CVE-2021-1919	https://www. qualcomm.co m/company/ product- security/bull etins/august- 2021-bulletin	H-QUA-QCA6- 170921/765
Integer Underflow (Wrap or Wraparoun d)	08-Sep-21	10	Integer underflow can occur due to improper handling of incoming RTCP packets in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Voice & Music, Snapdragon Wearables CVE ID : CVE-2021-1920	https://www. qualcomm.co m/company/ product- security/bull etins/august- 2021-bulletin	H-QUA-QCA6- 170921/766
Incorrect Type Conversion or Cast	08-Sep-21	4.6	Incorrect pointer argument passed to trusted application TA could result in un- intended memory operations in Snapdragon Auto,	https://www. qualcomm.co m/company/ product- security/bull	H-QUA-QCA6- 170921/767

CVSS Scoring Scale	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10
			Pa	age 279 c	of 1474					

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Snapdragon Compute, Snapdragon Connectivity, Snapdragon Industrial IOT CVE ID : CVE-2021-1923	etins/august- 2021-bulletin	
Exposure of Resource to Wrong Sphere	08-Sep-21	2.1	Lack of strict validation of bootmode can lead to information disclosure in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wearables	https://www. qualcomm.co m/company/ product- security/bull etins/august- 2021-bulletin	H-QUA-QCA6- 170921/768
Improper Restriction of Operations within the Bounds of a Memory Buffer	08-Sep-21	3.6	CVE ID : CVE-2021-1929 Possible out of bounds read due to incorrect validation of incoming buffer length in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile CVE ID : CVE-2021-1930	https://www. qualcomm.co m/company/ product- security/bull etins/august- 2021-bulletin	H-QUA-QCA6- 170921/769
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	08-Sep-21	10	Possible buffer overflow due to improper validation of device types during P2P search in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Woice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and	https://www. qualcomm.co m/company/ product- security/bull etins/august- 2021-bulletin	H-QUA-QCA6- 170921/770

0-1

1-2

7-8

5-6

6-7

8-9

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Networking		
			CVE ID : CVE-2021-1972		
qca6420					
Exposure of Resource to Wrong Sphere	08-Sep-21	2.1	Child process can leak information from parent process due to numeric pids are getting compared and these pid can be reused in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wearables CVE ID : CVE-2021-1904	https://www. qualcomm.co m/company/ product- security/bull etins/august- 2021-bulletin	H-QUA-QCA6- 170921/771
Loop with Unreachable Exit Condition ('Infinite Loop')	08-Sep-21	5	Loop with unreachable exit condition may occur due to improper handling of unsupported input in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Voice & Music, Snapdragon Wearables CVE ID : CVE-2021-1914	https://www. qualcomm.co m/company/ product- security/bull etins/august- 2021-bulletin	H-QUA-QCA6- 170921/772
Out-of- bounds Write	08-Sep-21	10	Possible buffer underflow due to lack of check for negative indices values when processing user provided input in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT,	https://www. qualcomm.co m/company/ product- security/bull etins/august- 2021-bulletin	H-QUA-QCA6- 170921/773
CVSS Scoring Sc	ale 0-1	1-2	2-3 3-4 4-5 5-6	6-7 7-8	8-9 9-10

Page 281 of 1474

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Voice & Music, Snapdragon Wearables		
			CVE ID : CVE-2021-1916		
Integer Underflow (Wrap or Wraparoun d)	08-Sep-21	10	Integer underflow can occur when the RTCP length is lesser than than the actual blocks present in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Voice & Music, Snapdragon Wearables CVE ID : CVE-2021-1919	https://www. qualcomm.co m/company/ product- security/bull etins/august- 2021-bulletin	H-QUA-QCA6- 170921/774
Integer Underflow (Wrap or Wraparoun d)	08-Sep-21	10	Integer underflow can occur due to improper handling of incoming RTCP packets in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Voice & Music, Snapdragon Wearables CVE ID : CVE-2021-1920	https://www. qualcomm.co m/company/ product- security/bull etins/august- 2021-bulletin	H-QUA-QCA6- 170921/775
			Incorrect pointer argument		
Incorrect Type Conversion or Cast	08-Sep-21	4.6	passed to trusted application TA could result in un- intended memory operations in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Industrial IOT CVE ID : CVE-2021-1923	https://www. qualcomm.co m/company/ product- security/bull etins/august- 2021-bulletin	H-QUA-QCA6- 170921/776
CVSS Scoring Sc	ale 0-1	1-2	2-3 3-4 4-5 5-6 Page 282 of 1474	6-7 7-8	8-9 9-10

Page 282 of 1474

Exposure of Resource to Wrong Sphere08-Sep-21Lack of strict validation of bootmode can lead to information disclosure in Snapdragon Auto, Snapdragon Consumer 10T, Snapdragon Industrial 10T, Snapdragon Industrial 10T, Snapdragon Consumer 10T, Snapdragon Industrial 10T, Snapdragon Consumer 10T, Snapdragon Mobile, Snapdragon Mobile, Snapdragon Consumer 10T, Snapdragon Mobile, Snapdragon Consumer 10T, Snapdragon Mobile, Snapdragon Consumer 10T, Snapdragon Mobile CVE 10 : CVE-2021-1930H-QUA-QCA6- H-QUA-QCA6- 100 Snapdragon Consumer 10T, Snapdragon Mobile, Snapdragon Mobile, Snapdragon Mobile, Snapdragon Mobile, Snapdragon Mobile, Snapdragon Mobile, Snapdragon Mobile, Snapdragon Mobile, Snapdragon Mobile, Snapdragon Wired Infrastructure and Networking CVE ID : CVE-2021-1972H-QUA-QCA6- H-QUA-QCA6- 10021/779Exposure of08-Sep-2108-Sep-2110Child process can leakhttps://www. H-QUA-QCA6- 10021-CVE-2021-1972	Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Improper Restriction of Operations within the Bounds of a Memory Buffer08-Sep-213.6due to incorrect validation of incoming buffer length in Snapdragon Compute, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobilehttps://www. qualcomm.co m/company/ product- security/bull etins/august- 2021-bulletinH-QUA-QCA6- 170921/778Buffer08-Sep-213.6Possible buffer overflow due to improper validation of device types during P2P search in Snapdragon Consumer IOT, Snapdragon Consumer IOT, Snapdragon Consumer IOT, Snapdragon Consumer IOT, Snapdragon MobileH-QUA-QCA6- 170921/778Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')08-Sep-21Possible buffer overflow due to improper validation of device types during P2P search in Snapdragon Consumer IOT, Snapdragon Consumer IOT, Snapdragon Mobile, Snapdragon Mobile, Snapdragon Mobile, Snapdragon Mobile, Snapdragon Mobile, Snapdragon Mobile, Snapdragon Wear Angdragon Wired Infrastructure and Networking CVE ID : CVE-2021-1972H-QUA-QCA6- 170921/779gca6421Exposure of08-Sep-212.1Child process can leakhttps://www.H-QUA-QCA6- 170921/779	Resource to Wrong	08-Sep-21	2.1	bootmode can lead to information disclosure in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wearables	qualcomm.co m/company/ product- security/bull etins/august-	
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')08-Sep-21to improper validation of device types during P2P search in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wied Infrastructure and Networkinghttps://www. qualcomm.co m/company/ product- security/bull etins/august- 2021-bulletinH-QUA-QCA6- 170921/779qca64212.1Child process can leakhttps://www.H-QUA-QCA6- 170921/779	Restriction of Operations within the Bounds of a Memory	08-Sep-21	3.6	due to incorrect validation of incoming buffer length in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile	qualcomm.co m/company/ product- security/bull etins/august-	
Exposure of 08-Sep-21 2.1 Child process can leak https://www. H-QUA-QCA6-	without Checking Size of Input ('Classic Buffer	08-Sep-21	10	to improper validation of device types during P2P search in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Woice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking	qualcomm.co m/company/ product- security/bull etins/august-	
	qca6421					
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
Resource to Wrong Sphere			information from parent process due to numeric pids are getting compared and these pid can be reused in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wearables CVE ID : CVE-2021-1904	qualcomm.co m/company/ product- security/bull etins/august- 2021-bulletin	170921/780
Loop with Unreachable Exit Condition ('Infinite Loop')	08-Sep-21	5	Loop with unreachable exit condition may occur due to improper handling of unsupported input in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Voice & Music, Snapdragon Wearables CVE ID : CVE-2021-1914	https://www. qualcomm.co m/company/ product- security/bull etins/august- 2021-bulletin	H-QUA-QCA6- 170921/781
Out-of- bounds Write	08-Sep-21	10	Possible buffer underflow due to lack of check for negative indices values when processing user provided input in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Voice & Music, Snapdragon Wearables	https://www. qualcomm.co m/company/ product- security/bull etins/august- 2021-bulletin	H-QUA-QCA6- 170921/782

CVSS Scoring Scale	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10
Page 284 of 1/7/										

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2021-1916		
Integer Underflow (Wrap or Wraparoun d)	08-Sep-21	10	Integer underflow can occur when the RTCP length is lesser than than the actual blocks present in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Voice & Music, Snapdragon Wearables CVE ID : CVE-2021-1919	https://www. qualcomm.co m/company/ product- security/bull etins/august- 2021-bulletin	H-QUA-QCA6- 170921/783
Integer Underflow (Wrap or Wraparoun d)	08-Sep-21	10	Integer underflow can occur due to improper handling of incoming RTCP packets in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Voice & Music, Snapdragon Wearables CVE ID : CVE-2021-1920	https://www. qualcomm.co m/company/ product- security/bull etins/august- 2021-bulletin	H-QUA-QCA6- 170921/784
Incorrect Type Conversion or Cast	08-Sep-21	Incorrect pointer argument passed to trusted application TA could result in un- intended memory operations		https://www. qualcomm.co m/company/ product- security/bull etins/august- 2021-bulletin	H-QUA-QCA6- 170921/785
Exposure of Resource to Wrong Sphere CVSS Scoring Sc	08-Sep-21 ale 0-1	2.1	Lack of strict validation of bootmode can lead to information disclosure in Snapdragon Auto, 2-3 3-4 4-5 5-6	https://www. qualcomm.co m/company/ product-	H-QUA-QCA6- 170921/786 8-9 9-10

Page 285 of 1474

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID		
			Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wearables	security/bull etins/august- 2021-bulletin			
			CVE ID : CVE-2021-1929				
Improper Restriction of Operations within the Bounds of a Memory Buffer	08-Sep-21	3.6	Possible out of bounds read due to incorrect validation of incoming buffer length in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile CVE ID : CVE-2021-1930	https://www. qualcomm.co m/company/ product- security/bull etins/august- 2021-bulletin	H-QUA-QCA6- 170921/787		
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	08-Sep-21	10	Possible buffer overflow due to improper validation of device types during P2P search in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Industrial IOT, Snapdragon Woile, Snapdragon Woice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking CVE ID : CVE-2021-1972	https://www. qualcomm.co m/company/ product- security/bull etins/august- 2021-bulletin	H-QUA-QCA6- 170921/788		
qca6426							
Exposure of Resource to Wrong Sphere	08-Sep-21	2.1	Child process can leak information from parent process due to numeric pids are getting compared and these pid can be reused in	https://www. qualcomm.co m/company/ product- security/bull	H-QUA-QCA6- 170921/789		

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables CVE ID : CVE-2021-1904	etins/august- 2021-bulletin	
Loop with Unreachable Exit Condition ('Infinite Loop')	08-Sep-21	5	Loop with unreachable exit condition may occur due to improper handling of unsupported input in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Voice & Music, Snapdragon Wearables CVE ID : CVE-2021-1914	https://www. qualcomm.co m/company/ product- security/bull etins/august- 2021-bulletin	H-QUA-QCA6- 170921/790
Out-of- bounds Write	ounds 08-Sep-21 10 Vrite		Possible buffer underflow due to lack of check for negative indices values when processing user provided input in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Voice & Music, Snapdragon Wearables CVE ID : CVE-2021-1916	https://www. qualcomm.co m/company/ product- security/bull etins/august- 2021-bulletin	H-QUA-QCA6- 170921/791
Integer Underflow (Wrap or	08-Sep-21	10	Integer underflow can occur when the RTCP length is lesser than than the actual	https://www. qualcomm.co m/company/	H-QUA-QCA6- 170921/792

Γ	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
Wraparoun d)			blocks present in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Voice & Music, Snapdragon Wearables CVE ID : CVE-2021-1919	product- security/bull etins/august- 2021-bulletin	
Integer Underflow (Wrap or Wraparoun d)	08-Sep-21	10	Integer underflow can occur due to improper handling of incoming RTCP packets in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Voice & Music, Snapdragon Wearables CVE ID : CVE-2021-1920	https://www. qualcomm.co m/company/ product- security/bull etins/august- 2021-bulletin	H-QUA-QCA6- 170921/793
Incorrect Type Conversion or Cast	08-Sep-21	4.6	Incorrect pointer argument passed to trusted application TA could result in un- intended memory operations in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Industrial IOT CVE ID : CVE-2021-1923	https://www. qualcomm.co m/company/ product- security/bull etins/august- 2021-bulletin	H-QUA-QCA6- 170921/794
Exposure of Resource to Wrong Sphere	08-Sep-21	2.1	Lack of strict validation of bootmode can lead to information disclosure in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT,	https://www. qualcomm.co m/company/ product- security/bull etins/august- 2021-bulletin	H-QUA-QCA6- 170921/795

0-1

1-2

5-6

6-7

7-8

8-9

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Snapdragon Mobile, Snapdragon Wearables CVE ID : CVE-2021-1929		
Improper Restriction of Operations within the Bounds of a Memory Buffer	08-Sep-21	3.6	Possible out of bounds read due to incorrect validation of incoming buffer length in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile CVE ID : CVE-2021-1930	https://www. qualcomm.co m/company/ product- security/bull etins/august- 2021-bulletin	H-QUA-QCA6- 170921/796
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	08-Sep-21	10	Possible buffer overflow due to improper validation of device types during P2P search in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Woice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking CVE ID : CVE-2021-1972	https://www. qualcomm.co m/company/ product- security/bull etins/august- 2021-bulletin	H-QUA-QCA6- 170921/797
qca6428					
Out-of- bounds Read	08-Sep-21	3.6	Buffer over read could occur due to incorrect check of buffer size while flashing emmc devices in Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon	https://www. qualcomm.co m/company/ product- security/bull etins/august- 2021-bulletin	H-QUA-QCA6- 170921/798
CVSS Scoring Sc	ale 0-1	1-2	Music, Snapdragon 2-3 3-4 4-5 5-6	6-7 7-8	8-9 9-:

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Wearables, Snapdragon Wired Infrastructure and Networking CVE ID : CVE-2021-1928		
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	08-Sep-21	10	Possible buffer overflow due to improper validation of device types during P2P search in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Woice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking CVE ID : CVE-2021-1972	https://www. qualcomm.co m/company/ product- security/bull etins/august- 2021-bulletin	H-QUA-QCA6- 170921/799
qca6430					
Exposure of Resource to Wrong Sphere	08-Sep-21	2.1	Child process can leak information from parent process due to numeric pids are getting compared and these pid can be reused in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wearables CVE ID : CVE-2021-1904	https://www. qualcomm.co m/company/ product- security/bull etins/august- 2021-bulletin	H-QUA-QCA6- 170921/800
Loop with Unreachable Exit Condition	08-Sep-21	5	Loop with unreachable exit condition may occur due to improper handling of unsupported input in	https://www. qualcomm.co m/company/ product-	H-QUA-QCA6- 170921/801
CVSS Scoring Sc	ale 0-1	1-2	2-3 3-4 4-5 5-6	6-7 7-8	8-9 9-10

Page 290 of 1474

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
('Infinite Loop')			Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Voice & Music, Snapdragon Wearables	security/bull etins/august- 2021-bulletin	
Out-of- bounds Write	08-Sep-21	10	CVE ID : CVE-2021-1914 Possible buffer underflow due to lack of check for negative indices values when processing user provided input in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Voice & Music, Snapdragon Wearables CVE ID : CVE-2021-1916	https://www. qualcomm.co m/company/ product- security/bull etins/august- 2021-bulletin	H-QUA-QCA6- 170921/802
Integer Underflow (Wrap or Wraparoun d)	08-Sep-21	10	Integer underflow can occur when the RTCP length is lesser than than the actual blocks present in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Voice & Music, Snapdragon Wearables CVE ID : CVE-2021-1919	https://www. qualcomm.co m/company/ product- security/bull etins/august- 2021-bulletin	H-QUA-QCA6- 170921/803
Integer Underflow (Wrap or Wraparoun	08-Sep-21	10	Integer underflow can occur due to improper handling of incoming RTCP packets in Snapdragon Auto,	https://www. qualcomm.co m/company/ product-	H-QUA-QCA6- 170921/804

CVSS Scoring Scale	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10
Dec. 201 (1171										

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
d)			Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Voice & Music, Snapdragon Wearables CVE ID : CVE-2021-1920	security/bull etins/august- 2021-bulletin	
Incorrect Type Conversion or Cast	08-Sep-21	4.6	Incorrect pointer argument passed to trusted application TA could result in un- intended memory operations in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Industrial IOT CVE ID : CVE-2021-1923	https://www. qualcomm.co m/company/ product- security/bull etins/august- 2021-bulletin	H-QUA-QCA6- 170921/805
Exposure of Resource to Wrong Sphere	08-Sep-21	2.1	Lack of strict validation of bootmode can lead to information disclosure in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wearables CVE ID : CVE-2021-1929	https://www. qualcomm.co m/company/ product- security/bull etins/august- 2021-bulletin	H-QUA-QCA6- 170921/806
Improper Restriction of Operations within the Bounds of a Memory Buffer	08-Sep-21	3.6	Possible out of bounds read due to incorrect validation of incoming buffer length in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile CVE ID : CVE-2021-1930	https://www. qualcomm.co m/company/ product- security/bull etins/august- 2021-bulletin	H-QUA-QCA6- 170921/807
CVSS Scoring Sco	ale 0-1	1-2	2-3 3-4 4-5 5-6 Page 292 of 1474	6-7 7-8	8-9 9-10

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	08-Sep-21	10	Possible buffer overflow due to improper validation of device types during P2P search in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Woice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking CVE ID : CVE-2021-1972	https://www. qualcomm.co m/company/ product- security/bull etins/august- 2021-bulletin	H-QUA-QCA6- 170921/808
qca6431				· ·	
Exposure of Resource to Wrong Sphere	08-Sep-21	2.1	Child process can leak information from parent process due to numeric pids are getting compared and these pid can be reused in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables CVE ID : CVE-2021-1904	https://www. qualcomm.co m/company/ product- security/bull etins/august- 2021-bulletin	H-QUA-QCA6- 170921/809
Loop with Unreachable Exit Condition ('Infinite Loop')	08-Sep-21	5	Loop with unreachable exit condition may occur due to improper handling of unsupported input in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT,	https://www. qualcomm.co m/company/ product- security/bull etins/august- 2021-bulletin	H-QUA-QCA6- 170921/810

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Snapdragon IoT, Snapdragon Voice & Music, Snapdragon Wearables		
			CVE ID : CVE-2021-1914		
Out-of- bounds Write	08-Sep-21	10	Possible buffer underflow due to lack of check for negative indices values when processing user provided input in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Voice & Music, Snapdragon Wearables	https://www. qualcomm.co m/company/ product- security/bull etins/august- 2021-bulletin	H-QUA-QCA6- 170921/811
			CVE ID : CVE-2021-1916		
Integer Underflow (Wrap or Wraparoun d)	08-Sep-21	10	Integer underflow can occur when the RTCP length is lesser than than the actual blocks present in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Voice & Music, Snapdragon Wearables	https://www. qualcomm.co m/company/ product- security/bull etins/august- 2021-bulletin	H-QUA-QCA6- 170921/812
			CVE ID : CVE-2021-1919		
Integer Underflow (Wrap or Wraparoun d)	08-Sep-21	10	Integer underflow can occur due to improper handling of incoming RTCP packets in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon	https://www. qualcomm.co m/company/ product- security/bull etins/august- 2021-bulletin	H-QUA-QCA6- 170921/813

1-2 2-3

0-1

5-6

6-7

7-8

8-9

Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
		Voice & Music, Snapdragon Wearables		
		CVE ID : CVE-2021-1920		
08-Sep-21	4.6	Incorrect pointer argument passed to trusted application TA could result in un- intended memory operations in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Industrial IOT CVE ID : CVE-2021-1923	https://www. qualcomm.co m/company/ product- security/bull etins/august- 2021-bulletin	H-QUA-QCA6- 170921/814
08-Sep-21	2.1	Lack of strict validation of bootmode can lead to information disclosure in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wearables	https://www. qualcomm.co m/company/ product- security/bull etins/august- 2021-bulletin	H-QUA-QCA6- 170921/815
08-Sep-21	3.6	Possible out of bounds read due to incorrect validation of incoming buffer length in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile CVE ID : CVE-2021-1930	https://www. qualcomm.co m/company/ product- security/bull etins/august- 2021-bulletin	H-QUA-QCA6- 170921/816
08-Sep-21	10	Possible buffer overflow due to improper validation of device types during P2P search in Snapdragon Auto, Snapdragon Compute,	https://www. qualcomm.co m/company/ product- security/bull	H-QUA-QCA6- 170921/817
	08-Sep-21 08-Sep-21	Image: marrier of the second secon	Image: constraint of the second sec	Image: Note of the section of the s

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Buffer Overflow')			Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking CVE ID : CVE-2021-1972	etins/august- 2021-bulletin	
qca6436				1	
Exposure of Resource to Wrong Sphere	08-Sep-21	2.1	Child process can leak information from parent process due to numeric pids are getting compared and these pid can be reused in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables CVE ID : CVE-2021-1904	https://www. qualcomm.co m/company/ product- security/bull etins/august- 2021-bulletin	H-QUA-QCA6- 170921/818
Loop with Unreachable Exit Condition ('Infinite Loop')	08-Sep-21	5	Loop with unreachable exit condition may occur due to improper handling of unsupported input in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Voice & Music, Snapdragon Wearables CVE ID : CVE-2021-1914	https://www. qualcomm.co m/company/ product- security/bull etins/august- 2021-bulletin	H-QUA-QCA6- 170921/819
CVSS Scoring Sc	ale 0-1	1-2	2-3 3-4 4-5 5-6	6-7 7-8	8-9 9-10

 3-4
 4-5
 5-6

 Page 296 of 1474

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Out-of- bounds Write	08-Sep-21	10	Possible buffer underflow due to lack of check for negative indices values when processing user provided input in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Voice & Music, Snapdragon Wearables CVE ID : CVE-2021-1916	https://www. qualcomm.co m/company/ product- security/bull etins/august- 2021-bulletin	H-QUA-QCA6- 170921/820
Integer Underflow (Wrap or Wraparoun d)	08-Sep-21	10	Integer underflow can occur when the RTCP length is lesser than than the actual blocks present in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Voice & Music, Snapdragon Wearables CVE ID : CVE-2021-1919	https://www. qualcomm.co m/company/ product- security/bull etins/august- 2021-bulletin	H-QUA-QCA6- 170921/821
Integer Underflow (Wrap or Wraparoun d)	08-Sep-21	10	Integer underflow can occur due to improper handling of incoming RTCP packets in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Voice & Music, Snapdragon Wearables	https://www. qualcomm.co m/company/ product- security/bull etins/august- 2021-bulletin	H-QUA-QCA6- 170921/822
Incorrect	08-Sep-21	4.6	CVE ID : CVE-2021-1920 Incorrect pointer argument	https://www.	H-QUA-QCA6-
	-				\ \

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Type Conversion or Cast			passed to trusted application TA could result in un- intended memory operations in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Industrial IOT CVE ID : CVE-2021-1923	qualcomm.co m/company/ product- security/bull etins/august- 2021-bulletin	170921/823
Exposure of Resource to Wrong Sphere	08-Sep-21	2.1	Lack of strict validation of bootmode can lead to information disclosure in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wearables CVE ID : CVE-2021-1929	https://www. qualcomm.co m/company/ product- security/bull etins/august- 2021-bulletin	H-QUA-QCA6- 170921/824
Improper Restriction of Operations within the Bounds of a Memory Buffer	08-Sep-21	3.6	Possible out of bounds read due to incorrect validation of incoming buffer length in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile CVE ID : CVE-2021-1930	https://www. qualcomm.co m/company/ product- security/bull etins/august- 2021-bulletin	H-QUA-QCA6- 170921/825
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	08-Sep-21	10	Possible buffer overflow due to improper validation of device types during P2P search in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile,	https://www. qualcomm.co m/company/ product- security/bull etins/august- 2021-bulletin	H-QUA-QCA6- 170921/826

0-1

1-2

5-6

6-7

7-8

8-9

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking		
qca6438			CVE ID : CVE-2021-1972		
Out-of- bounds Read	08-Sep-21	3.6	Buffer over read could occur due to incorrect check of buffer size while flashing emmc devices in Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and	https://www. qualcomm.co m/company/ product- security/bull etins/august- 2021-bulletin	H-QUA-QCA6- 170921/827
			Networking CVE ID : CVE-2021-1928		
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	08-Sep-21	10	Possible buffer overflow due to improper validation of device types during P2P search in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Woice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking CVE ID : CVE-2021-1972	https://www. qualcomm.co m/company/ product- security/bull etins/august- 2021-bulletin	H-QUA-QCA6- 170921/828
qca6564				-	
Exposure of Resource to	08-Sep-21	2.1	Child process can leak information from parent	https://www. qualcomm.co	H-QUA-QCA6-
CVSS Scoring Sc	cale 0-1	1-2	2-3 3-4 4-5 5-6 Page 299 of 1474	6-7 7-8	8-9 9-10

Sphereare getting compared and these pid can be reused in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer 10T, Snapdragon Consumer 10T, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearablesproduct- security/bull etins/august- 2021-bulletinBuffer Copy without Checking Size of Input (Classic Buffer Overflow')08-Sep-21Possible buffer overflow due to improper validation of device types during P2P search in Snapdragon Consumer 10T, Snapdragon Connectivity, Snapdragon Connuctivity, Snapdragon Consumer 10T, Snapdragon Mobile, Snapdragon Consumer 10T, Snapdragon Wired Infrastructure and Networking CVE ID : CVE-2021-1972https://www. qualcomm.co m/company/ product- security/bull etins/august- 2021-bulletinqca6564aChild process can leak information from parent process due to numeric pids are getting compared and these pid can be reused in Snapdragon Connuctivity, Snapdragon Consumer 10T, Snapdragon Consumer 10T, Snapdragon Que Snapdragon Wired Information from parent process due to numeric pids are getting compared and these pid can be reused in Snapdragon Connuctivity, Snapdragon Consumer 10T, Snapdragon Consumer 10T, Snapd	Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')08-Sep-21Image: Comparison of the security of	-			are getting compared and these pid can be reused in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables	product- security/bull etins/august-	170921/829
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')08-Sep-2110to improper validation of device types during P2P search in Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Mobile, Snapdragon Voice & Music, Overflow')https://www. qualcomm.co m/company/ product- security/bull etins/august- 2021-bulletinH-QUA-Q 170921/ etins/august- 2021-bulletin qca6564a 08-Sep-212.1Child process can leak information from parent process due to numeric pids are getting compared and these pid can be reused in Snapdragon Connectivity, Snapdragon Connectivity, Snapdragon Connectivity, Snapdragon Wired Infrastructure and Networkinghttps://www. qualcomm.co 						
qca6564aqca6564aExposure of Resource to Wrong SphereResep-21Child process can leak information from parent process due to numeric pids are getting compared and these pid can be reused in Snapdragon Auto, Snapdragon Connectivity, Snapdragon Connectivity, Snapdragon Consumer IOT,https://www. qualcomm.co m/company/ product- security/bull etins/august- 2021-bulletinH-QUA-Q 170921/	without Checking Size of Input ('Classic Buffer	08-Sep-21	10	to improper validation of device types during P2P search in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Woice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking	qualcomm.co m/company/ product- security/bull etins/august-	H-QUA-QCA6- 170921/830
Exposure of Resource to Wrong Sphere08-Sep-21Child process can leak information from parent process due to numeric pids are getting compared and these pid can be reused in Snapdragon Auto, Snapdragon Connectivity, Snapdragon Consumer IOT,https://www. qualcomm.co m/company/ product- security/bull etins/august- 2021-bulletinH-QUA-Q 170921/ H-QUA-Q URA-Q DRA-Q URA-Q DRA-Q URA-Q	aaa6564a			CVE ID : CVE-2021-1972		
Snapdragon Mobile,	Exposure of Resource to Wrong	08-Sep-21	2.1	information from parent process due to numeric pids are getting compared and these pid can be reused in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT,	qualcomm.co m/company/ product- security/bull etins/august-	H-QUA-QCA6- 170921/831

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Snapdragon Voice & Music, Snapdragon Wearables		
			CVE ID : CVE-2021-1904		
Loop with Unreachable Exit Condition ('Infinite Loop')	08-Sep-21	5	Loop with unreachable exit condition may occur due to improper handling of unsupported input in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Voice & Music, Snapdragon Wearables CVE ID : CVE-2021-1914	https://www. qualcomm.co m/company/ product- security/bull etins/august- 2021-bulletin	H-QUA-QCA6- 170921/832
Out-of- bounds Write	08-Sep-21	10	Possible buffer underflow due to lack of check for negative indices values when processing user provided input in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Voice & Music, Snapdragon Wearables CVE ID : CVE-2021-1916	https://www. qualcomm.co m/company/ product- security/bull etins/august- 2021-bulletin	H-QUA-QCA6- 170921/833
Integer Underflow (Wrap or Wraparoun d)	08-Sep-21	10	Integer underflow can occur when the RTCP length is lesser than than the actual blocks present in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon	https://www. qualcomm.co m/company/ product- security/bull etins/august- 2021-bulletin	H-QUA-QCA6- 170921/834

0-1

1-2

2-3 3-4 4-5 Page 301 of 1474 6-7

5-6

7-8

8-9

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Voice & Music, Snapdragon Wearables		
			CVE ID : CVE-2021-1919		
Integer Underflow (Wrap or Wraparoun d)	08-Sep-21	10	Integer underflow can occur due to improper handling of incoming RTCP packets in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Voice & Music, Snapdragon Wearables	https://www. qualcomm.co m/company/ product- security/bull etins/august- 2021-bulletin	H-QUA-QCA6- 170921/835
			CVE ID : CVE-2021-1920		
Exposure of Resource to Wrong Sphere	08-Sep-21	2.1	Lack of strict validation of bootmode can lead to information disclosure in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wearables CVE ID : CVE-2021-1929	https://www. qualcomm.co m/company/ product- security/bull etins/august- 2021-bulletin	H-QUA-QCA6- 170921/836
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	08-Sep-21	10	Possible buffer overflow due to improper validation of device types during P2P search in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Woice & Music, Snapdragon Wearables, Snapdragon Wired	https://www. qualcomm.co m/company/ product- security/bull etins/august- 2021-bulletin	H-QUA-QCA6- 170921/837

0-1

1-2

2-3 3-4

4-5

6-7

5-6

7-8

8-9

qca6564aupca65	8-Sep-21		Infrastructure and Networking CVE ID : CVE-2021-1972 Child process can leak information from parent process due to numeric pids are getting compared and these pid can be reused in Snandragon Auto		
Exposure of Resource to Wrong 08	8-Sep-21		CVE ID : CVE-2021-1972 Child process can leak information from parent process due to numeric pids are getting compared and these pid can be reused in		
Exposure of Resource to Wrong 08	8-Sep-21		Child process can leak information from parent process due to numeric pids are getting compared and these pid can be reused in		
Exposure of Resource to Wrong 08	8-Sep-21		information from parent process due to numeric pids are getting compared and these pid can be reused in		
Resource to Wrong 08	8-Sep-21		information from parent process due to numeric pids are getting compared and these pid can be reused in		
		2.1	Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables CVE ID : CVE-2021-1904	https://www. qualcomm.co m/company/ product- security/bull etins/august- 2021-bulletin	H-QUA-QCA6- 170921/838
Loop with Unreachable Exit Condition ('Infinite Loop')	8-Sep-21	5	Loop with unreachable exit condition may occur due to improper handling of unsupported input in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Voice & Music, Snapdragon Wearables CVE ID : CVE-2021-1914	https://www. qualcomm.co m/company/ product- security/bull etins/august- 2021-bulletin	H-QUA-QCA6- 170921/839
Out-of- bounds 08 Write	8-Sep-21	10	Possible buffer underflow due to lack of check for negative indices values when processing user provided input in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity,	https://www. qualcomm.co m/company/ product- security/bull etins/august- 2021-bulletin	H-QUA-QCA6- 170921/840

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Voice & Music, Snapdragon Wearables CVE ID : CVE-2021-1916		
Integer Underflow (Wrap or Wraparoun d)	08-Sep-21	10	Integer underflow can occur when the RTCP length is lesser than than the actual blocks present in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Voice & Music, Snapdragon Wearables CVE ID : CVE-2021-1919	https://www. qualcomm.co m/company/ product- security/bull etins/august- 2021-bulletin	H-QUA-QCA6- 170921/841
Integer Underflow (Wrap or Wraparoun d)	08-Sep-21	10	Integer underflow can occur due to improper handling of incoming RTCP packets in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Voice & Music, Snapdragon Wearables CVE ID : CVE-2021-1920	https://www. qualcomm.co m/company/ product- security/bull etins/august- 2021-bulletin	H-QUA-QCA6- 170921/842
Exposure of Resource to Wrong Sphere	08-Sep-21	2.1	Lack of strict validation of bootmode can lead to information disclosure in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT,	https://www. qualcomm.co m/company/ product- security/bull etins/august- 2021-bulletin	H-QUA-QCA6- 170921/843

0-1

1-2 2-3 3-4

4-5

5-6

6-7

7-8

8-9

Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
		Snapdragon Mobile, Snapdragon Wearables CVE ID : CVE-2021-1929		
08-Sep-21	3.6	Possible out of bounds read due to incorrect validation of incoming buffer length in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile CVE ID : CVE-2021-1930	https://www. qualcomm.co m/company/ product- security/bull etins/august- 2021-bulletin	H-QUA-QCA6- 170921/844
08-Sep-21	10	Possible buffer overflow due to improper validation of device types during P2P search in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Woice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking CVE ID : CVE-2021-1972	https://www. qualcomm.co m/company/ product- security/bull etins/august- 2021-bulletin	H-QUA-QCA6- 170921/845
<u> </u>	<u> </u>		<u> </u>	
08-Sep-21	2.1	Child process can leak information from parent process due to numeric pids are getting compared and these pid can be reused in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT,	https://www. qualcomm.co m/company/ product- security/bull etins/august- 2021-bulletin	H-QUA-QCA6- 170921/846
	08-Sep-21	Image: marrier of the series of the serie	Image: construct of the second seco	Image: constraint of the standard of the stand

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables		
			CVE ID : CVE-2021-1904		
Loop with Unreachable Exit Condition ('Infinite Loop')	08-Sep-21	5	Loop with unreachable exit condition may occur due to improper handling of unsupported input in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Voice & Music, Snapdragon Wearables	https://www. qualcomm.co m/company/ product- security/bull etins/august- 2021-bulletin	H-QUA-QCA6- 170921/847
			CVE ID : CVE-2021-1914		
Out-of- bounds Write	08-Sep-21	10	Possible buffer underflow due to lack of check for negative indices values when processing user provided input in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Voice & Music, Snapdragon Wearables CVE ID : CVE-2021-1916	https://www. qualcomm.co m/company/ product- security/bull etins/august- 2021-bulletin	H-QUA-QCA6- 170921/848
Integer Underflow (Wrap or Wraparoun d)	08-Sep-21	10	Integer underflow can occur when the RTCP length is lesser than than the actual blocks present in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT,	https://www. qualcomm.co m/company/ product- security/bull etins/august- 2021-bulletin	H-QUA-QCA6- 170921/849
CVSS Scoring Sc	ale 0-1	1-2	2-3 3-4 4-5 5-6 Page 306 of 1474	6-7 7-8	8-9 9-10

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Voice & Music, Snapdragon Wearables		
			CVE ID : CVE-2021-1919		
Integer Underflow (Wrap or Wraparoun d)	08-Sep-21	10	Integer underflow can occur due to improper handling of incoming RTCP packets in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Voice & Music, Snapdragon Wearables CVE ID : CVE-2021-1920	https://www. qualcomm.co m/company/ product- security/bull etins/august- 2021-bulletin	H-QUA-QCA6- 170921/850
Incorrect Type Conversion or Cast	08-Sep-21	4.6	Incorrect pointer argument passed to trusted application TA could result in un- intended memory operations in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Industrial IOT CVE ID : CVE-2021-1923	https://www. qualcomm.co m/company/ product- security/bull etins/august- 2021-bulletin	H-QUA-QCA6- 170921/851
Improper Restriction of Operations within the Bounds of a Memory Buffer	08-Sep-21	3.6	Possible out of bounds read due to incorrect validation of incoming buffer length in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile CVE ID : CVE-2021-1930	https://www. qualcomm.co m/company/ product- security/bull etins/august- 2021-bulletin	H-QUA-QCA6- 170921/852
Buffer Copy without CVSS Scoring Sc	08-Sep-21	10	Possible buffer overflow due to improper validation of 2-3 3-4 4-5 5-6	https://www. qualcomm.co	H-QUA-QCA6- 8-9 9-10

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Checking Size of Input ('Classic Buffer Overflow')			device types during P2P search in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Woice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking CVE ID : CVE-2021-1972	m/company/ product- security/bull etins/august- 2021-bulletin	170921/853
qca6574a					
Exposure of Resource to Wrong Sphere	08-Sep-21	2.1	Child process can leak information from parent process due to numeric pids are getting compared and these pid can be reused in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables CVE ID : CVE-2021-1904	https://www. qualcomm.co m/company/ product- security/bull etins/august- 2021-bulletin	H-QUA-QCA6- 170921/854
Loop with Unreachable Exit Condition ('Infinite Loop')	08-Sep-21	5	Loop with unreachable exit condition may occur due to improper handling of unsupported input in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Voice & Music, Snapdragon	https://www. qualcomm.co m/company/ product- security/bull etins/august- 2021-bulletin	H-QUA-QCA6- 170921/855

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Wearables		
			CVE ID : CVE-2021-1914		
Out-of- bounds Write	08-Sep-21	10	Possible buffer underflow due to lack of check for negative indices values when processing user provided input in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Voice & Music, Snapdragon Wearables	https://www. qualcomm.co m/company/ product- security/bull etins/august- 2021-bulletin	H-QUA-QCA6- 170921/856
			CVE ID : CVE-2021-1916		
Integer Underflow (Wrap or Wraparoun d)	08-Sep-21	10	Integer underflow can occur when the RTCP length is lesser than than the actual blocks present in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Voice & Music, Snapdragon Wearables CVE ID : CVE-2021-1919	https://www. qualcomm.co m/company/ product- security/bull etins/august- 2021-bulletin	H-QUA-QCA6- 170921/857
Integer Underflow (Wrap or Wraparoun d)	08-Sep-21	10	Integer underflow can occur due to improper handling of incoming RTCP packets in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Voice & Music, Snapdragon Wearables	https://www. qualcomm.co m/company/ product- security/bull etins/august- 2021-bulletin	H-QUA-QCA6- 170921/858
CVSS Scoring Sco	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-2021-1920		
Incorrect Type Conversion or Cast	08-Sep-21	4.6	Incorrect pointer argument passed to trusted application TA could result in un- intended memory operations in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Industrial IOT CVE ID : CVE-2021-1923	https://www. qualcomm.co m/company/ product- security/bull etins/august- 2021-bulletin	H-QUA-QCA6- 170921/859
Exposure of Resource to Wrong Sphere	08-Sep-21	2.1	Lack of strict validation of bootmode can lead to information disclosure in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wearables CVE ID : CVE-2021-1929	https://www. qualcomm.co m/company/ product- security/bull etins/august- 2021-bulletin	H-QUA-QCA6- 170921/860
Improper Restriction of Operations within the Bounds of a Memory Buffer	08-Sep-21	3.6	Possible out of bounds read due to incorrect validation of incoming buffer length in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile CVE ID : CVE-2021-1930	https://www. qualcomm.co m/company/ product- security/bull etins/august- 2021-bulletin	H-QUA-QCA6- 170921/861
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	08-Sep-21	10	Possible buffer overflow due to improper validation of device types during P2P search in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT,	https://www. qualcomm.co m/company/ product- security/bull etins/august- 2021-bulletin	H-QUA-QCA6- 170921/862

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking		
qca6574au			CVE ID : CVE-2021-1972		
Exposure of Resource to Wrong Sphere	08-Sep-21	2.1	Child process can leak information from parent process due to numeric pids are getting compared and these pid can be reused in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables CVE ID : CVE-2021-1904	https://www. qualcomm.co m/company/ product- security/bull etins/august- 2021-bulletin	H-QUA-QCA6- 170921/863
Loop with Unreachable Exit Condition ('Infinite Loop')	08-Sep-21	5	Loop with unreachable exit condition may occur due to improper handling of unsupported input in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Voice & Music, Snapdragon Wearables CVE ID : CVE-2021-1914	https://www. qualcomm.co m/company/ product- security/bull etins/august- 2021-bulletin	H-QUA-QCA6- 170921/864
Out-of- bounds	08-Sep-21	10	Possible buffer underflow due to lack of check for	https://www. qualcomm.co	H-QUA-QCA6- 170921/865

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Write			negative indices values when processing user provided input in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Voice & Music, Snapdragon Wearables CVE ID : CVE-2021-1916	m/company/ product- security/bull etins/august- 2021-bulletin	
Integer Underflow (Wrap or Wraparoun d)	08-Sep-21	10	Integer underflow can occur when the RTCP length is lesser than than the actual blocks present in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Voice & Music, Snapdragon Wearables CVE ID : CVE-2021-1919	https://www. qualcomm.co m/company/ product- security/bull etins/august- 2021-bulletin	H-QUA-QCA6- 170921/866
Integer Underflow (Wrap or Wraparoun d)	08-Sep-21	10	Integer underflow can occur due to improper handling of incoming RTCP packets in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Voice & Music, Snapdragon Wearables	https://www. qualcomm.co m/company/ product- security/bull etins/august- 2021-bulletin	H-QUA-QCA6- 170921/867
Incorrect	08-Sep-21	4.6	CVE ID : CVE-2021-1920 Incorrect pointer argument passed to trusted application	https://www.	H-QUA-QCA6-
Type Conversion		10	TA could result in un-	qualcomm.co m/company/	170921/868

CVSS Scoring Scale	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10
			P	age 312 c	of 1474					

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
or Cast			intended memory operations in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Industrial IOT CVE ID : CVE-2021-1923	product- security/bull etins/august- 2021-bulletin	
Exposure of Resource to Wrong Sphere	08-Sep-21	2.1	Lack of strict validation of bootmode can lead to information disclosure in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wearables CVE ID : CVE-2021-1929	https://www. qualcomm.co m/company/ product- security/bull etins/august- 2021-bulletin	H-QUA-QCA6- 170921/869
Improper Restriction of Operations within the Bounds of a Memory Buffer	08-Sep-21	3.6	Possible out of bounds read due to incorrect validation of incoming buffer length in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile CVE ID : CVE-2021-1930	https://www. qualcomm.co m/company/ product- security/bull etins/august- 2021-bulletin	H-QUA-QCA6- 170921/870
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	08-Sep-21	10	Possible buffer overflow due to improper validation of device types during P2P search in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables,	https://www. qualcomm.co m/company/ product- security/bull etins/august- 2021-bulletin	H-QUA-QCA6- 170921/871

1-2 2-3

0-1

4-5

6-7

5-6

7-8

8-9

9-10

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Snapdragon Wired Infrastructure and Networking		
			CVE ID : CVE-2021-1972		
qca6584					
Exposure of Resource to Wrong Sphere	08-Sep-21	2.1	Child process can leak information from parent process due to numeric pids are getting compared and these pid can be reused in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wearables CVE ID : CVE-2021-1904	https://www. qualcomm.co m/company/ product- security/bull etins/august- 2021-bulletin	H-QUA-QCA6- 170921/872
Loop with Unreachable Exit Condition ('Infinite Loop')	08-Sep-21	5	Loop with unreachable exit condition may occur due to improper handling of unsupported input in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Voice & Music, Snapdragon Wearables CVE ID : CVE-2021-1914	https://www. qualcomm.co m/company/ product- security/bull etins/august- 2021-bulletin	H-QUA-QCA6- 170921/873
Out-of- bounds Write	08-Sep-21	10	Possible buffer underflow due to lack of check for negative indices values when processing user provided input in Snapdragon Auto, Snapdragon Compute,	https://www. qualcomm.co m/company/ product- security/bull etins/august-	H-QUA-QCA6- 170921/874
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 & CVE ID	Patch	NCIIPC ID
			Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Voice & Music, Snapdragon Wearables	2021-bulletin	
			CVE ID : CVE-2021-1916		
Integer Underflow (Wrap or Wraparoun d)	08-Sep-21	10	Integer underflow can occur due to improper handling of incoming RTCP packets in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Voice & Music, Snapdragon Wearables	https://www. qualcomm.co m/company/ product- security/bull etins/august- 2021-bulletin	H-QUA-QCA6- 170921/875
			CVE ID : CVE-2021-1920		
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	08-Sep-21	10	Possible buffer overflow due to improper validation of device types during P2P search in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Woice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking CVE ID : CVE-2021-1972	https://www. qualcomm.co m/company/ product- security/bull etins/august- 2021-bulletin	H-QUA-QCA6- 170921/876
qca6584au				.	
Exposure of Resource to Wrong	08-Sep-21	2.1	Child process can leak information from parent process due to numeric pids	https://www. qualcomm.co m/company/	H-QUA-QCA6- 170921/877
CVSS Scoring Sc	ale 0-1	1-2	2-3 3-4 4-5 5-6 Page 315 of 1474	6-7 7-8	8-9 9-10

Page 315 of 1474

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Sphere			are getting compared and these pid can be reused in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wearables CVE ID : CVE-2021-1904	product- security/bull etins/august- 2021-bulletin	
Loop with Unreachable Exit Condition ('Infinite Loop')	08-Sep-21	5	Loop with unreachable exit condition may occur due to improper handling of unsupported input in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Voice & Music, Snapdragon Wearables CVE ID : CVE-2021-1914	https://www. qualcomm.co m/company/ product- security/bull etins/august- 2021-bulletin	H-QUA-QCA6- 170921/878
Out-of- bounds Write	08-Sep-21	10	Possible buffer underflow due to lack of check for negative indices values when processing user provided input in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Voice & Music, Snapdragon Wearables CVE ID : CVE-2021-1916	https://www. qualcomm.co m/company/ product- security/bull etins/august- 2021-bulletin	H-QUA-QCA6- 170921/879
Integer	08-Sep-21	10	Integer underflow can occur	https://www.	H-QUA-QCA6-

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Underflow (Wrap or Wraparoun d)			when the RTCP length is lesser than than the actual blocks present in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Voice & Music, Snapdragon Wearables CVE ID : CVE-2021-1919	qualcomm.co m/company/ product- security/bull etins/august- 2021-bulletin	170921/880
Integer Underflow (Wrap or Wraparoun d)	08-Sep-21	10	Integer underflow can occur due to improper handling of incoming RTCP packets in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Voice & Music, Snapdragon Wearables CVE ID : CVE-2021-1920	https://www. qualcomm.co m/company/ product- security/bull etins/august- 2021-bulletin	H-QUA-QCA6- 170921/881
Improper Restriction of Operations within the Bounds of a Memory Buffer	08-Sep-21	3.6	Possible out of bounds read due to incorrect validation of incoming buffer length in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile CVE ID : CVE-2021-1930	https://www. qualcomm.co m/company/ product- security/bull etins/august- 2021-bulletin	H-QUA-QCA6- 170921/882
Buffer Copy without Checking Size of Input ('Classic	08-Sep-21	10	Possible buffer overflow due to improper validation of device types during P2P search in Snapdragon Auto, Snapdragon Compute,	https://www. qualcomm.co m/company/ product- security/bull	H-QUA-QCA6- 170921/883

0-1

1-2

2-3 3-4 4-5 Page 317 of 1474 7-8

5-6

6-7

8-9

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Buffer Overflow')			Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking CVE ID : CVE-2021-1972	etins/august- 2021-bulletin	
qca6595	I			<u> </u>	I
Exposure of Resource to Wrong Sphere	08-Sep-21	2.1	Child process can leak information from parent process due to numeric pids are getting compared and these pid can be reused in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wearables CVE ID : CVE-2021-1904	https://www. qualcomm.co m/company/ product- security/bull etins/august- 2021-bulletin	H-QUA-QCA6- 170921/884
Incorrect Type Conversion or Cast	08-Sep-21	4.6	Incorrect pointer argument passed to trusted application TA could result in un- intended memory operations in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Industrial IOT CVE ID : CVE-2021-1923	https://www. qualcomm.co m/company/ product- security/bull etins/august- 2021-bulletin	H-QUA-QCA6- 170921/885
Exposure of Resource to Wrong Sphere CVSS Scoring Sc	08-Sep-21	2.1	Lack of strict validation of bootmode can lead to information disclosure in Snapdragon Auto, 2-3 3-4 4-5 5-6	https://www. qualcomm.co m/company/ product-	H-QUA-QCA6- 170921/886 8-9 9-10

Page 318 of 1474

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wearables	security/bull etins/august- 2021-bulletin	
			CVE ID : CVE-2021-1929		
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	08-Sep-21	10	Possible buffer overflow due to improper validation of device types during P2P search in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Woice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking CVE ID : CVE-2021-1972	https://www. qualcomm.co m/company/ product- security/bull etins/august- 2021-bulletin	H-QUA-QCA6- 170921/887
qca6595au					
Exposure of Resource to Wrong Sphere	08-Sep-21	2.1	Child process can leak information from parent process due to numeric pids are getting compared and these pid can be reused in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music,	https://www. qualcomm.co m/company/ product- security/bull etins/august- 2021-bulletin	H-QUA-QCA6- 170921/888
			Snapdragon Wearables CVE ID : CVE-2021-1904		

		condition may occur due to	qualcomm.co	170921/889
		improper handling of unsupported input in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Voice & Music, Snapdragon Wearables	m/company/ product- security/bull etins/august- 2021-bulletin	1709217009
		CVE ID : CVE-2021-1914		
)8-Sep-21	10	Possible buffer underflow due to lack of check for negative indices values when processing user provided input in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Voice & Music, Snapdragon Wearables	https://www. qualcomm.co m/company/ product- security/bull etins/august- 2021-bulletin	H-QUA-QCA6- 170921/890
		CVE ID : CVE-2021-1916		
)8-Sep-21	10	Integer underflow can occur when the RTCP length is lesser than than the actual blocks present in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Voice & Music, Snapdragon Wearables CVE ID : CVE-2021-1919	https://www. qualcomm.co m/company/ product- security/bull etins/august- 2021-bulletin	H-QUA-QCA6- 170921/891
)8-Sep-21	10	Integer underflow can occur	https://www.	H-QUA-QCA6-
)	- 18-Sep-21	- 98-Sep-21 10	8-Sep-2110Snapdragon Connectivity, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Voice & Music, Snapdragon Wearables8-Sep-2110Possible buffer underflow due to lack of check for negative indices values when processing user provided input in Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Voice & Music, Snapdragon Voice & Music, Snapdragon Wearables8-Sep-21108-Sep-211010Integer underflow can occur when the RTCP length is lesser than than the actual blocks present in Snapdragon Auto, Snapdragon Consumer IOT, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Consumer IOT, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Industrial IOT, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Voice & Music, Snapdragon Voice & Mu	8-Sep-2110Snapdragon Connectivity, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Voice & Music, Snapdragon Wearables2021-bulletin8-Sep-2110Possible buffer underflow due to lack of check for negative indices values when processing user provided input in Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Industrial IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Voice & Music, Snapdragon NearablesHttps://www. qualcomm.co m/company/ product- security/bull etins/august- 2021-bulletin8-Sep-2110Integer underflow can occur when the RTCP length is lesser than than the actual blocks present in Snapdragon Auto, Snapdragon Conmetivity, Snapdragon Consumer IOT, Snapdragon IoT, Snapdragon Auto, Snapdragon Conmetivity, Snapdragon IoT, Snapdragon Voice & Music,

Page 320 of 1474

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Underflow (Wrap or Wraparoun d)			due to improper handling of incoming RTCP packets in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Voice & Music, Snapdragon Wearables CVE ID : CVE-2021-1920	qualcomm.co m/company/ product- security/bull etins/august- 2021-bulletin	170921/892
Incorrect Type Conversion or Cast	08-Sep-21	4.6	Incorrect pointer argument passed to trusted application TA could result in un- intended memory operations in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Industrial IOT CVE ID : CVE-2021-1923	https://www. qualcomm.co m/company/ product- security/bull etins/august- 2021-bulletin	H-QUA-QCA6- 170921/893
Exposure of Resource to Wrong Sphere	08-Sep-21	2.1	Lack of strict validation of bootmode can lead to information disclosure in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wearables CVE ID : CVE-2021-1929	https://www. qualcomm.co m/company/ product- security/bull etins/august- 2021-bulletin	H-QUA-QCA6- 170921/894
Improper Restriction of Operations within the Bounds of a Memory	08-Sep-21	3.6	Possible out of bounds read due to incorrect validation of incoming buffer length in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT,	https://www. qualcomm.co m/company/ product- security/bull etins/august- 2021-bulletin	H-QUA-QCA6- 170921/895

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Buffer			Snapdragon Industrial IOT, Snapdragon Mobile CVE ID : CVE-2021-1930		
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	08-Sep-21	10	Possible buffer overflow due to improper validation of device types during P2P search in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Woice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking	https://www. qualcomm.co m/company/ product- security/bull etins/august- 2021-bulletin	H-QUA-QCA6- 170921/896
			CVE ID : CVE-2021-1972		
qca6694			I 11 1 1 1		
Loop with Unreachable Exit Condition ('Infinite Loop')	08-Sep-21	5	Loop with unreachable exit condition may occur due to improper handling of unsupported input in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Voice & Music, Snapdragon Wearables CVE ID : CVE-2021-1914	https://www. qualcomm.co m/company/ product- security/bull etins/august- 2021-bulletin	H-QUA-QCA6- 170921/897
			Possible buffer underflow	https://www.	
Out-of- bounds Write	08-Sep-21	10	due to lack of check for negative indices values when processing user provided input in Snapdragon Auto, Snapdragon Compute,	qualcomm.co m/company/ product- security/bull etins/august-	H-QUA-QCA6- 170921/898
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 & CVE ID	Patch	NCIIPC ID		
			Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Voice & Music, Snapdragon Wearables	2021-bulletin			
			CVE ID : CVE-2021-1916				
Integer Underflow (Wrap or Wraparoun d)	08-Sep-21	10	Integer underflow can occur when the RTCP length is lesser than than the actual blocks present in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Voice & Music, Snapdragon Wearables	https://www. qualcomm.co m/company/ product- security/bull etins/august- 2021-bulletin	H-QUA-QCA6- 170921/899		
			CVE ID : CVE-2021-1919				
Integer Underflow (Wrap or Wraparoun d)	08-Sep-21	10	Integer underflow can occur due to improper handling of incoming RTCP packets in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Voice & Music, Snapdragon Wearables CVE ID : CVE-2021-1920	https://www. qualcomm.co m/company/ product- security/bull etins/august- 2021-bulletin	H-QUA-QCA6- 170921/900		
Out-of- bounds Read	08-Sep-21	3.6	Buffer over read could occur due to incorrect check of buffer size while flashing emmc devices in Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon	https://www. qualcomm.co m/company/ product- security/bull etins/august- 2021-bulletin	H-QUA-QCA6- 170921/901		
CVSS Scoring Scale 0-1 1-2 2-3 3-4 4-5 5-6 6-7 7-8 8-9 9-10 Page 323 of 1474							

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID			
			Mobile, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking CVE ID : CVE-2021-1928					
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	08-Sep-21	10	Possible buffer overflow due to improper validation of device types during P2P search in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Woice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking CVE ID : CVE-2021-1972	https://www. qualcomm.co m/company/ product- security/bull etins/august- 2021-bulletin	H-QUA-QCA6- 170921/902			
qca6694au								
Loop with Unreachable Exit Condition ('Infinite Loop')	08-Sep-21	5	Loop with unreachable exit condition may occur due to improper handling of unsupported input in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Voice & Music, Snapdragon Wearables CVE ID : CVE-2021-1914	https://www. qualcomm.co m/company/ product- security/bull etins/august- 2021-bulletin	H-QUA-QCA6- 170921/903			
Out-of- bounds Write	08-Sep-21	10	Possible buffer underflow due to lack of check for negative indices values when	https://www. qualcomm.co m/company/	H-QUA-QCA6- 170921/904			
CVSS Scoring Scale 0-1 1-2 2-3 3-4 4-5 5-6 6-7 7-8 8-9 9-10 Page 324 of 1474								

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID	
			processing user provided input in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Voice & Music, Snapdragon Wearables CVE ID : CVE-2021-1916	product- security/bull etins/august- 2021-bulletin		
Integer Underflow (Wrap or Wraparoun d)	08-Sep-21	10	Integer underflow can occur when the RTCP length is lesser than than the actual blocks present in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Voice & Music, Snapdragon Wearables CVE ID : CVE-2021-1919	https://www. qualcomm.co m/company/ product- security/bull etins/august- 2021-bulletin	H-QUA-QCA6- 170921/905	
Integer Underflow (Wrap or d)08-Sep-2110Integer underflow can occur due to improper handling of incoming RTCP packets in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Industrial IOT, Snapdragon Industrial IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Voice & Music, Snapdragon Voice & Music, Snapdragonhttps://www. qualcomm.co m/company/ product- security/bull etins/august- 2021-bulletinH-QUA-QCA6- 10021/906						
qca6696						
Exposure of Resource to Wrong	08-Sep-21	2.1	Child process can leak information from parent process due to numeric pids	https://www. qualcomm.co m/company/	H-QUA-QCA6- 170921/907	
CVSS Scoring Sca	ale 0-1	1-2	2-3 3-4 4-5 5-6 Page 325 of 1474	6-7 7-8	8-9 9-10	

Page 325 of 1474

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID		
Sphere			are getting compared and these pid can be reused in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables CVE ID : CVE-2021-1904	product- security/bull etins/august- 2021-bulletin			
Loop with Unreachable Exit ConditionLoop with unreachable exit condition may occur due to improper handling ofhttps://www. qualcomm.co m/company/ product- security/bull etins/august- 2021-bulletinH-QI 170908-Sep-2155Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Wearableshttps://www. product- security/bull etins/august- 2021-bulletinH-QI 1709							
Out-of- bounds08-Sep-2110Possible buffer underflow due to lack of check for negative indices values when processing user provided Snapdragon Compute, Snapdragon Connectivity, Snapdragon Industrial IOT, Snapdragon Industrial IOT, Snapdragon Industrial IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Voice & Music, Snapdragon Wearableshttps://www. qualcomm.co m/company/ product- security/bull etins/august- 2021-bulletinH-QUA- 170921							
Integer08-Sep-2110Integer underflow can occurhttps://www.H-QUA-QCA6-							

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Underflow (Wrap or Wraparoun d)			when the RTCP length is lesser than than the actual blocks present in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Voice & Music, Snapdragon Wearables CVE ID : CVE-2021-1919	qualcomm.co m/company/ product- security/bull etins/august- 2021-bulletin	170921/910
Integer Underflow (Wrap or Wraparoun d)	08-Sep-21	10	Integer underflow can occur due to improper handling of incoming RTCP packets in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Voice & Music, Snapdragon Wearables CVE ID : CVE-2021-1920	https://www. qualcomm.co m/company/ product- security/bull etins/august- 2021-bulletin	H-QUA-QCA6- 170921/911
Incorrect Type Conversion or Cast	08-Sep-21	4.6	Incorrect pointer argument passed to trusted application TA could result in un- intended memory operations in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Industrial IOT CVE ID : CVE-2021-1923	https://www. qualcomm.co m/company/ product- security/bull etins/august- 2021-bulletin	H-QUA-QCA6- 170921/912
Exposure of Resource to Wrong Sphere	08-Sep-21	2.1	Lack of strict validation of bootmode can lead to information disclosure in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity,	https://www. qualcomm.co m/company/ product- security/bull etins/august-	H-QUA-QCA6- 170921/913

0-1

1-2 2-3

3-4

4-5

5-6

6-7

7-8

8-9

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID		
			Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wearables	2021-bulletin			
			CVE ID : CVE-2021-1929				
Improper Restriction of Operations within the Bounds of a Memory Buffer	08-Sep-21	3.6	Possible out of bounds read due to incorrect validation of incoming buffer length in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile	https://www. qualcomm.co m/company/ product- security/bull etins/august- 2021-bulletin	H-QUA-QCA6- 170921/914		
			CVE ID : CVE-2021-1930				
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	08-Sep-21	10	Possible buffer overflow due to improper validation of device types during P2P search in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Woice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking CVE ID : CVE-2021-1972	https://www. qualcomm.co m/company/ product- security/bull etins/august- 2021-bulletin	H-QUA-QCA6- 170921/915		
qca7500							
Out-of- bounds Read	08-Sep-21	3.6	Buffer over read could occur due to incorrect check of buffer size while flashing emmc devices in Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon	https://www. qualcomm.co m/company/ product- security/bull etins/august- 2021-bulletin	H-QUA-QCA7- 170921/916		
CVSS Scoring Sc	ale 0-1	1-2	2-3 3-4 4-5 5-6 Page 328 of 1474	6-7 7-8	8-9 9-10		

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID		
			Mobile, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking				
			CVE ID : CVE-2021-1928				
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	08-Sep-21	10	Possible buffer overflow due to improper validation of device types during P2P search in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Woice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking CVE ID : CVE-2021-1972	https://www. qualcomm.co m/company/ product- security/bull etins/august- 2021-bulletin	H-QUA-QCA7- 170921/917		
qca7520							
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')Possible buffer overflow due to improper validation of device types during P2P search in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wired Infrastructure and Networkinghttps://www. H-QUA-QCA7- 170921/918U08-Sep-2110Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Voice & Music, Snapdragon Wired Infrastructure and NetworkingH-QUA-QCA7- 170921/918							
qca7550							
CVSS Scoring Sc	ale 0-1	1-2	2-3 3-4 4-5 5-6 Page 329 of 1474	6-7 7-8	8-9 9-10		

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	08-Sep-21	10	Possible buffer overflow due to improper validation of device types during P2P search in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Woice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking CVE ID : CVE-2021-1972	https://www. qualcomm.co m/company/ product- security/bull etins/august- 2021-bulletin	H-QUA-QCA7- 170921/919
qca8072	I			l	
Out-of- bounds 08-Sep-21 3.6 Read		Buffer over read could occur due to incorrect check of buffer size while flashing emmc devices in Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking CVE ID : CVE-2021-1928	https://www. qualcomm.co m/company/ product- security/bull etins/august- 2021-bulletin	H-QUA-QCA8- 170921/920	
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow') 08-Sep-21 10 ('CVSS Scoring Scale 0-1 1-2		10	Possible buffer overflow due to improper validation of device types during P2P search in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music,	https://www. qualcomm.co m/company/ product- security/bull etins/august- 2021-bulletin	H-QUA-QCA8- 170921/921

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID				
			Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking						
			CVE ID : CVE-2021-1972						
qca8075	qca8075								
Out-of- bounds Read	bounds 08-Sep-21 3.6 Industrial IOT, Snapdragon product- H-QUA-QCA8- 170921/922								
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	08-Sep-21	10	Possible buffer overflow due to improper validation of device types during P2P search in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Woice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking CVE ID : CVE-2021-1972	https://www. qualcomm.co m/company/ product- security/bull etins/august- 2021-bulletin	H-QUA-QCA8- 170921/923				
qca8081					-				
Out-of- bounds	08-Sep-21	3.6	Buffer over read could occur due to incorrect check of buffer size while flashing	https://www. qualcomm.co m/company/	H-QUA-QCA8- 170921/924				
CVSS Scoring Sc	ale 0-1	1-2	2-3 3-4 4-5 5-6 Page 331 of 1474	6-7 7-8	8-9 <mark>9-10</mark>				

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Read	Connectivity, Consumer IO Industrial IO Mobile, Snapo Music, Snapd Wearables, Sn Wired Infrast Networking		emmc devices in Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking CVE ID : CVE-2021-1928	product- security/bull etins/august- 2021-bulletin	
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	08-Sep-21	10	Possible buffer overflow due to improper validation of device types during P2P search in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Woice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking CVE ID : CVE-2021-1972	https://www. qualcomm.co m/company/ product- security/bull etins/august- 2021-bulletin	H-QUA-QCA8- 170921/925
qca8337					
Exposure of Resource to Wrong Sphere	08-Sep-21	2.1	Child process can leak information from parent process due to numeric pids are getting compared and these pid can be reused in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music,	https://www. qualcomm.co m/company/ product- security/bull etins/august- 2021-bulletin	H-QUA-QCA8- 170921/926

CVSS Scoring Scale	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10
			Pa	age 332 c	of 1474					

Size of input ('Classic Buffer Overflow')08-Sep-2110Snapdragon Mobile, Snapdragon Wied Infrastructure and Networking CVE ID : CVE-2021-1972product- security/bull etins/august- 2021-bulletin170921/927qca9367CVE ID : CVE-2021-19722021-bulletin170921/927qca9367Child process can leak information from parent process due to numeric pids are getting compared and these pid can be reused in Snapdragon Connectivity, Snapdragon Connectivity, Snapdragon Mobile, Snapdragon Mobile, Snapdragon Mobile, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Mobile, Snapdragon Noice & Music, Snapdragon NearablesH-QUA-QCA9- 170921/928Exposure of Resource to Wrong Sphere08-Sep-212.1Child process can leak information from parent process due to numeric pids are getting compared and these pid can be reused in Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Nobile, Snapdragon Nobile, Snapdragon Nobile, Snapdragon Nobile, Snapdragon Nobile, Snapdragon Nobile, Snapdragon Wearables CVE ID : CVE-2021-1904H-QUA-QCA9- 170921/928Loop with UnreachableLoop with unreachable exit condition may occur due tohttps://www. qualcomm.co	Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Buffer Copy without Checking Size of Input (Classic Buffer Overflow')Possible buffer overflow due to improper validation of device types during P2P search in Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Nobile, Snapdragon Wired Infrastructure and Networking CVE ID : CVE-2021-1972https://www. qualcomm.co m/company/ product- security/bull etins/august- 2021-bulletinH-QUA-QCA8- 10021/927qca936708-Sep-212.1Child process can leak information from parent process due to numeric pids are gettig compared and these pid can be reused in Snapdragon Consumer IOT, Snapdragon Consumer IOT, Snapdragon Outed Infrastructure and NetworkingH-QUA-QCA8- 10021/927qca93672.1Child process can leak information from parent process due to numeric pids are gettig compared and these pid can be reused in Snapdragon Consumer IOT, Snapdragon Consumer IOT, Snapdragon Consumer IOT, Snapdragon Consumer IOT, Snapdragon Consumer IOT, Snapdragon Consumer IOT, Snapdragon Mobile, Snapdragon Mobile, Snapdragon Mobile, Snapdragon Mobile, Snapdragon Netoce & Music, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Voice & Music, Snapdragon Voice & Music, Snapdragon Voice & Music, Snapdragon Wearables CVE ID : CVE-2021-1904H-QUA-QCA9- H-QUA-QCA9- 170921/928Loop with Unreachable Exit Condition (Infinite08-Sep-215Loop with unreachable exit condition may occur due to improper handling of unsupported input in Snapdragon Auto,https://www. qualcomm.co m/company/ product- security/bullLoop with Unreachable Exit Condition (Infini				Snapdragon Wearables		
Buffer Copy without Checking Size of Input (Classic Buffer Cov')08-Sep-21to improper validation of device types during P2P search in Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Consumer IOT, Snapdragon Mobile, Snapdragon Mobile, Snapdragon Wearables, Snapdragon Wired information from parent process due to numeric pids are getting compared and these pid can be reused in Snapdragon Consumer IOT, Snapdragon Mobile, Snapdragon Consumer IOT, Snapdragon Consumer IOT, Snapdragon Consumer IOT, Snapdragon Consumer IOT, Snapdragon Consumer IOT, Snapdragon Nobile, Snapdragon Nobile, Snapd				CVE ID : CVE-2021-1904		
Exposure of Resource to Wrong Sphere08-Sep-212.1Child process can leak information from parent process due to numeric pids are getting compared and these pid can be reused in Snapdragon Auto, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Consumer IOT, Snapdragon Mobile, Snapdragon Wearableshttps://www. qualcomm.co m/company/ product- security/bull etins/august- 2021-bulletinH-QUA-QCA9- 170921/928Loop with Unreachable Exit Condition ('Infinite08-Sep-215Loop with unreachable exit improper handling of snapdragon Auto,https://www. qualcomm.co m/company/ product- security/bull etins/august- 2021-bulletinH-QUA-QCA9- 170921/928	without Checking Size of Input ('Classic Buffer	08-Sep-21	10	to improper validation of device types during P2P search in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Woice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking	qualcomm.co m/company/ product- security/bull etins/august-	H-QUA-QCA8- 170921/927
Exposure of Resource to Wrong Sphere08-Sep-212.1information from parent process due to numeric pids are getting compared and these pid can be reused in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wearableshttps://www. qualcomm.co m/company/ product- security/bull etins/august- 2021-bulletinH-QUA-QCA9- 170921/928Loop with Unreachable Exit Condition ('Infinite08-Sep-215Loop with unreachable exit condition may occur due to improper handling of unsupported input in Snapdragon Auto,https://www. qualcomm.co m/company/ product- security/bull	qca9367					
Unreachable Exit Condition ('Infinite08-Sep-215condition may occur due to improper handling of unsupported input in Snapdragon Auto,qualcomm.co m/company/ product- security/bullH-QUA-QCA9- 170921/929	Resource to Wrong 08-Sep-21 2.1			information from parent process due to numeric pids are getting compared and these pid can be reused in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wearables	qualcomm.co m/company/ product- security/bull etins/august-	H-QUA-QCA9- 170921/928
	Unreachable Exit Condition ('Infinite	08-Sep-21	5	condition may occur due to improper handling of unsupported input in Snapdragon Auto,	qualcomm.co m/company/ product- security/bull	H-QUA-QCA9- 170921/929

Page 333 of 1474

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Voice & Music, Snapdragon Wearables	2021-bulletin	
			CVE ID : CVE-2021-1914		
Out-of- bounds Write	08-Sep-21	10	Possible buffer underflow due to lack of check for negative indices values when processing user provided input in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Voice & Music, Snapdragon Wearables CVE ID : CVE-2021-1916	https://www. qualcomm.co m/company/ product- security/bull etins/august- 2021-bulletin	H-QUA-QCA9- 170921/930
Integer Underflow (Wrap or Wraparoun d)	08-Sep-21	10	Integer underflow can occur when the RTCP length is lesser than than the actual blocks present in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Voice & Music, Snapdragon Wearables CVE ID : CVE-2021-1919	https://www. qualcomm.co m/company/ product- security/bull etins/august- 2021-bulletin	H-QUA-QCA9- 170921/931
Integer Underflow (Wrap or Wraparoun d)	08-Sep-21	10	Integer underflow can occur due to improper handling of incoming RTCP packets in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity,	https://www. qualcomm.co m/company/ product- security/bull etins/august-	H-QUA-QCA9- 170921/932

0-1

1-2

5-6

6-7

7-8

8-9

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Voice & Music, Snapdragon Wearables	2021-bulletin	
			CVE ID : CVE-2021-1920		
Out-of- bounds Read	08-Sep-21	3.6	Buffer over read could occur due to incorrect check of buffer size while flashing emmc devices in Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking	https://www. qualcomm.co m/company/ product- security/bull etins/august- 2021-bulletin	H-QUA-QCA9- 170921/933
			CVE ID : CVE-2021-1928		
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	08-Sep-21	10	Possible buffer overflow due to improper validation of device types during P2P search in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Industrial IOT, Snapdragon Woice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking CVE ID : CVE-2021-1972	https://www. qualcomm.co m/company/ product- security/bull etins/august- 2021-bulletin	H-QUA-QCA9- 170921/934
qca9377					
Exposure of Resource to Wrong	08-Sep-21	2.1	Child process can leak information from parent process due to numeric pids	https://www. qualcomm.co m/company/	H-QUA-QCA9- 170921/935
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 & CVE ID	Patch	NCIIPC ID
Sphere			are getting compared and these pid can be reused in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables CVE ID : CVE-2021-1904	product- security/bull etins/august- 2021-bulletin	
Loop with Unreachable Exit Condition ('Infinite Loop')	08-Sep-21	5	Loop with unreachable exit condition may occur due to improper handling of unsupported input in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Voice & Music, Snapdragon Wearables CVE ID : CVE-2021-1914	https://www. qualcomm.co m/company/ product- security/bull etins/august- 2021-bulletin	H-QUA-QCA9- 170921/936
Out-of- bounds Write	08-Sep-21	10	Possible buffer underflow due to lack of check for negative indices values when processing user provided input in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Voice & Music, Snapdragon Wearables CVE ID : CVE-2021-1916	https://www. qualcomm.co m/company/ product- security/bull etins/august- 2021-bulletin	H-QUA-QCA9- 170921/937
	08-Sep-21	10	Integer underflow can occur	https://www.	H-QUA-QCA9-

Page 336 of 1474

	 when the RTCP length is lesser than than the actual blocks present in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Voice & Music, Snapdragon Wearables CVE ID : CVE-2021-1919 Integer underflow can occur due to improper handling of 	qualcomm.co m/company/ product- security/bull etins/august- 2021-bulletin	170921/938
	U U		
p-21 10	 incoming RTCP packets in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Voice & Music, Snapdragon Wearables CVE ID : CVE-2021-1920 	https://www. qualcomm.co m/company/ product- security/bull etins/august- 2021-bulletin	H-QUA-QCA9- 170921/939
p-21 3.6	 Buffer over read could occur due to incorrect check of buffer size while flashing emmc devices in Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking CVE ID : CVE-2021-1928 	https://www. qualcomm.co m/company/ product- security/bull etins/august- 2021-bulletin	H-QUA-QCA9- 170921/940
21 2 (Possible out of bounds read due to incorrect validation of	https://www. qualcomm.co	H-QUA-QCA9- 170921/941
	p-21 3.6	 p-21 p-21 a.6 p-21 p-21 a.6 a.6 a.6 b.7 b.7 consumer IOT, Snapdragon Consumer IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking cve ID : cve-2021-1928 p-21 p-23 a.6 	p-21emmc devices in Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networkinghttps://www. qualcomm.co m/company/ product- security/bull etins/august- 2021-bulletinp-213.6Possible out of bounds read due to incorrect validation ofhttps://www. qualcomm.co

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
of Operations within the Bounds of a Memory Buffer			incoming buffer length in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile CVE ID : CVE-2021-1930	m/company/ product- security/bull etins/august- 2021-bulletin	
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	08-Sep-21	10	Possible buffer overflow due to improper validation of device types during P2P search in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Woice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking CVE ID : CVE-2021-1972	https://www. qualcomm.co m/company/ product- security/bull etins/august- 2021-bulletin	H-QUA-QCA9- 170921/942
qca9379					
Exposure of Resource to Wrong Sphere	08-Sep-21	2.1	Child process can leak information from parent process due to numeric pids are getting compared and these pid can be reused in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wearables CVE ID : CVE-2021-1904	https://www. qualcomm.co m/company/ product- security/bull etins/august- 2021-bulletin	H-QUA-QCA9- 170921/943
CVSS Scoring Sca	ale 0-1	1-2	2-3 3-4 4-5 5-6	6-7 7-8	8-9 9-10

Page 338 of 1474

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Loop with Unreachable Exit Condition ('Infinite Loop')	08-Sep-21	5	Loop with unreachable exit condition may occur due to improper handling of unsupported input in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Voice & Music, Snapdragon Wearables CVE ID : CVE-2021-1914	https://www. qualcomm.co m/company/ product- security/bull etins/august- 2021-bulletin	H-QUA-QCA9- 170921/944
Out-of- bounds Write	08-Sep-21	10	Possible buffer underflow due to lack of check for negative indices values when processing user provided input in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Voice & Music, Snapdragon Wearables CVE ID : CVE-2021-1916	https://www. qualcomm.co m/company/ product- security/bull etins/august- 2021-bulletin	H-QUA-QCA9- 170921/945
Integer Underflow (Wrap or Wraparoun d)	08-Sep-21	10	Integer underflow can occur when the RTCP length is lesser than than the actual blocks present in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Voice & Music, Snapdragon Wearables CVE ID : CVE-2021-1919	https://www. qualcomm.co m/company/ product- security/bull etins/august- 2021-bulletin	H-QUA-QCA9- 170921/946

CVSS Scoring Scale	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10
			D	200 220 0	f 1/7/					

Wraparoun d) Buffer Copy without Checking	Sep-21	10	Integer underflow can occur due to improper handling of incoming RTCP packets in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Voice & Music, Snapdragon	https://www. qualcomm.co m/company/ product- security/bull etins/august-	H-QUA-QCA9- 170921/947
without Checking Size of Input 08- ('Classic Buffer			Wearables	2021-bulletin	
without Checking Size of Input 08- ('Classic Buffer			CVE ID : CVE-2021-1920		
	Sep-21	10	Possible buffer overflow due to improper validation of device types during P2P search in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Woice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking CVE ID : CVE-2021-1972	https://www. qualcomm.co m/company/ product- security/bull etins/august- 2021-bulletin	H-QUA-QCA9- 170921/948
0524			CVE ID : CVE-2021-1972		
qca9531 Out-of- bounds 08- Read	Sep-21	3.6	Buffer over read could occur due to incorrect check of buffer size while flashing emmc devices in Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and	https://www. qualcomm.co m/company/ product- security/bull etins/august- 2021-bulletin	H-QUA-QCA9- 170921/949

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Networking CVE ID : CVE-2021-1928		
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	08-Sep-21	10	Possible buffer overflow due to improper validation of device types during P2P search in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Woice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking CVE ID : CVE-2021-1972	https://www. qualcomm.co m/company/ product- security/bull etins/august- 2021-bulletin	H-QUA-QCA9- 170921/950
qca9558					
Out-of- bounds Read	08-Sep-21	3.6	Buffer over read could occur due to incorrect check of buffer size while flashing emmc devices in Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking CVE ID : CVE-2021-1928	https://www. qualcomm.co m/company/ product- security/bull etins/august- 2021-bulletin	H-QUA-QCA9- 170921/951
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	08-Sep-21	10	Possible buffer overflow due to improper validation of device types during P2P search in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT,	https://www. qualcomm.co m/company/ product- security/bull etins/august- 2021-bulletin	H-QUA-QCA9- 170921/952
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 & CVE ID	Patch	NCIIPC ID
			Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking CVE ID : CVE-2021-1972		
qca9561					
Out-of- bounds Read	08-Sep-21	3.6	Buffer over read could occur due to incorrect check of buffer size while flashing emmc devices in Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking CVE ID : CVE-2021-1928	https://www. qualcomm.co m/company/ product- security/bull etins/august- 2021-bulletin	H-QUA-QCA9- 170921/953
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	08-Sep-21	10	Possible buffer overflow due to improper validation of device types during P2P search in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Woice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking CVE ID : CVE-2021-1972	https://www. qualcomm.co m/company/ product- security/bull etins/august- 2021-bulletin	H-QUA-QCA9- 170921/954
qca9563					
CVSS Scoring Sc	ale 0-1	1-2	2-3 3-4 4-5 5-6 Page 342 of 1474	6-7 7-8	8-9 9-10

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Out-of- bounds Read	08-Sep-21	3.6	Buffer over read could occur due to incorrect check of buffer size while flashing emmc devices in Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking CVE ID : CVE-2021-1928	https://www. qualcomm.co m/company/ product- security/bull etins/august- 2021-bulletin	H-QUA-QCA9- 170921/955
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	08-Sep-21	10	Possible buffer overflow due to improper validation of device types during P2P search in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Woice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking CVE ID : CVE-2021-1972	https://www. qualcomm.co m/company/ product- security/bull etins/august- 2021-bulletin	H-QUA-QCA9- 170921/956
qca9880					
Out-of- bounds Read	08-Sep-21	3.6	Buffer over read could occur due to incorrect check of buffer size while flashing emmc devices in Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon	https://www. qualcomm.co m/company/ product- security/bull etins/august- 2021-bulletin	H-QUA-QCA9- 170921/957

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Wired Infrastructure and Networking CVE ID : CVE-2021-1928		
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	08-Sep-21	10	Possible buffer overflow due to improper validation of device types during P2P search in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Woice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking CVE ID : CVE-2021-1972	https://www. qualcomm.co m/company/ product- security/bull etins/august- 2021-bulletin	H-QUA-QCA9- 170921/958
qca9882					
Out-of- bounds Read	08-Sep-21	3.6	Buffer over read could occur due to incorrect check of buffer size while flashing emmc devices in Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking CVE ID : CVE-2021-1928	https://www. qualcomm.co m/company/ product- security/bull etins/august- 2021-bulletin	H-QUA-QCA9- 170921/959
Buffer Copy without Checking Size of Input ('Classic Buffer	08-Sep-21	10	Possible buffer overflow due to improper validation of device types during P2P search in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity,	https://www. qualcomm.co m/company/ product- security/bull etins/august-	H-QUA-QCA9- 170921/960
CVSS Scoring Sc	ale 0-1	1-2	2-3 3-4 4-5 5-6	6-7 7-8	8-9 9-10

Page 344 of 1474

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Overflow')			Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking CVE ID : CVE-2021-1972	2021-bulletin	
qca9886	L			I	
Out-of- bounds Read	08-Sep-21	3.6	Buffer over read could occur due to incorrect check of buffer size while flashing emmc devices in Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking	https://www. qualcomm.co m/company/ product- security/bull etins/august- 2021-bulletin	H-QUA-QCA9- 170921/961
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	08-Sep-21	10	CVE ID : CVE-2021-1928 Possible buffer overflow due to improper validation of device types during P2P search in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Woice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking CVE ID : CVE-2021-1972	https://www. qualcomm.co m/company/ product- security/bull etins/august- 2021-bulletin	H-QUA-QCA9- 170921/962

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
qca9887				<u></u>	
Out-of- bounds Read	08-Sep-21	3.6	Buffer over read could occur due to incorrect check of buffer size while flashing emmc devices in Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking CVE ID : CVE-2021-1928	https://www. qualcomm.co m/company/ product- security/bull etins/august- 2021-bulletin	H-QUA-QCA9- 170921/963
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	08-Sep-21	10	Possible buffer overflow due to improper validation of device types during P2P search in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Woice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking CVE ID : CVE-2021-1972	https://www. qualcomm.co m/company/ product- security/bull etins/august- 2021-bulletin	H-QUA-QCA9- 170921/964
qca9888					
Out-of- bounds Read	08-Sep-21	3.6	Buffer over read could occur due to incorrect check of buffer size while flashing emmc devices in Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice &	https://www. qualcomm.co m/company/ product- security/bull etins/august- 2021-bulletin	H-QUA-QCA9- 170921/965

0-1

1-2

5-6

6-7

7-8

8-9

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking		
			CVE ID : CVE-2021-1928		
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	08-Sep-21	10	Possible buffer overflow due to improper validation of device types during P2P search in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Woice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking CVE ID : CVE-2021-1972	https://www. qualcomm.co m/company/ product- security/bull etins/august- 2021-bulletin	H-QUA-QCA9- 170921/966
qca9889					
Out-of- bounds Read	08-Sep-21	3.6	Buffer over read could occur due to incorrect check of buffer size while flashing emmc devices in Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking CVE ID : CVE-2021-1928	https://www. qualcomm.co m/company/ product- security/bull etins/august- 2021-bulletin	H-QUA-QCA9- 170921/967
Buffer Copy without Checking Size of Input	08-Sep-21	10	Possible buffer overflow due to improper validation of device types during P2P search in Snapdragon Auto,	https://www. qualcomm.co m/company/ product-	H-QUA-QCA9- 170921/968
CVSS Scoring Sc	ale 0-1	1-2	2-3 3-4 4-5 5-6	6-7 7-8	8-9 9-10

Page 347 of 1474

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
('Classic Buffer Overflow')			Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking CVE ID : CVE-2021-1972	security/bull etins/august- 2021-bulletin	
qca9896					
Out-of- bounds Read	08-Sep-21	3.6	Buffer over read could occur due to incorrect check of buffer size while flashing emmc devices in Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking CVE ID : CVE-2021-1928	https://www. qualcomm.co m/company/ product- security/bull etins/august- 2021-bulletin	H-QUA-QCA9- 170921/969
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	08-Sep-21	10	Possible buffer overflow due to improper validation of device types during P2P search in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Woice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and	https://www. qualcomm.co m/company/ product- security/bull etins/august- 2021-bulletin	H-QUA-QCA9- 170921/970

CVSS Scoring Scale	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10
			Р	age 348 c	of 1474					

)8-Sep-21	3.6	Networking CVE ID : CVE-2021-1972 Buffer over read could occur due to incorrect check of buffer size while flashing emmc devices in Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon	https://www. qualcomm.co	
)8-Sep-21	3.6	Buffer over read could occur due to incorrect check of buffer size while flashing emmc devices in Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon	qualcomm.co	
)8-Sep-21	3.6	due to incorrect check of buffer size while flashing emmc devices in Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon	qualcomm.co	
)8-Sep-21	3.6	due to incorrect check of buffer size while flashing emmc devices in Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon	qualcomm.co	
		Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking CVE ID : CVE-2021-1928	m/company/ product- security/bull etins/august- 2021-bulletin	H-QUA-QCA9- 170921/971
)8-Sep-21	10	Possible buffer overflow due to improper validation of device types during P2P search in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Woice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking CVE ID : CVE-2021-1972	https://www. qualcomm.co m/company/ product- security/bull etins/august- 2021-bulletin	H-QUA-QCA9- 170921/972
)8-Sep-21	3.6	Buffer over read could occur due to incorrect check of buffer size while flashing emmc devices in Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon	https://www. qualcomm.co m/company/ product- security/bull etins/august-	H-QUA-QCA9- 170921/973
	-	8-Sep-21 3.6	Wired Infrastructure and NetworkingCVE ID : CVE-2021-1928Possible buffer overflow due to improper validation of device types during P2P search in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wierd Infrastructure and Networking8-Sep-21108-Sep-21Supproved to the second	Wired Infrastructure and NetworkingHitps://www.CVE ID : CVE-2021-1928Possible buffer overflow due to improper validation of device types during P2P search in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Mobile, Snapdragon Mobile, Snapdragon Noice & Music, Snapdragon Wired Infrastructure and Networkinghttps://www. qualcomm.co m/company/ product- security/bull etins/august- 2021-bulletin8-Sep-2110Buffer over read could occur due to incorrect check of buffer size while flashing emmc devices in Snapdragon Connectivity, Snapdragon connectivity, Snapdragon connectivity, Snapdragon due to incorrect check of buffer size while flashing emmc devices in Snapdragon connectivity, Snapdragon connectivity, Snapdragon connectivity, Snapdragon consumer IOT, Snapdragonhttps://www. qualcomm.co m/company/ product- security/bull etins/august- 2021-bulletin

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking	2021-bulletin	
			CVE ID : CVE-2021-1928		
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	08-Sep-21	10	Possible buffer overflow due to improper validation of device types during P2P search in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Woice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking CVE ID : CVE-2021-1972	https://www. qualcomm.co m/company/ product- security/bull etins/august- 2021-bulletin	H-QUA-QCA9- 170921/974
qca9982					
Out-of- bounds Read	08-Sep-21	3.6	Buffer over read could occur due to incorrect check of buffer size while flashing emmc devices in Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking CVE ID : CVE-2021-1928	https://www. qualcomm.co m/company/ product- security/bull etins/august- 2021-bulletin	H-QUA-QCA9- 170921/975
Buffer Copy without	08-Sep-21	10	Possible buffer overflow due to improper validation of	https://www. qualcomm.co	H-QUA-QCA9- 170921/976

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Checking Size of Input ('Classic Buffer Overflow')			device types during P2P search in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Woice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking CVE ID : CVE-2021-1972	m/company/ product- security/bull etins/august- 2021-bulletin	
qca9984					
Out-of- bounds Read	08-Sep-21	3.6	Buffer over read could occur due to incorrect check of buffer size while flashing emmc devices in Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking	https://www. qualcomm.co m/company/ product- security/bull etins/august- 2021-bulletin	H-QUA-QCA9- 170921/977
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	hout cking of Input assic Fer		https://www. qualcomm.co m/company/ product- security/bull etins/august- 2021-bulletin	H-QUA-QCA9- 170921/978	

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID					
			Infrastructure and							
			Networking							
			CVE ID : CVE-2021-1972							
qca9985										
Out-of- bounds Read	08-Sep-21	3.6	Buffer over read could occur due to incorrect check of buffer size while flashing emmc devices in Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking CVE ID : CVE-2021-1928	https://www. qualcomm.co m/company/ product- security/bull etins/august- 2021-bulletin	H-QUA-QCA9- 170921/979					
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	08-Sep-21	10	Possible buffer overflow due to improper validation of device types during P2P search in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Woice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking CVE ID : CVE-2021-1972	https://www. qualcomm.co m/company/ product- security/bull etins/august- 2021-bulletin	H-QUA-QCA9- 170921/980					
qca9986										
Buffer Copy without Checking Size of Input ('Classic	08-Sep-21	10	Possible buffer overflow due to improper validation of device types during P2P search in Snapdragon Auto, Snapdragon Compute,	https://www. qualcomm.co m/company/ product- security/bull	H-QUA-QCA9- 170921/981					
CVSS Scoring Sc	ale 0-1	1-2	2-3 3-4 4-5 5-6 Page 352 of 1474	6-7 7-8	8-9 9-10					

Page 352 of 1474

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Buffer Overflow')			Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking CVE ID : CVE-2021-1972	etins/august- 2021-bulletin	
qca9987					
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	08-Sep-21	10	Possible buffer overflow due to improper validation of device types during P2P search in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Woice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking CVE ID : CVE-2021-1972	https://www. qualcomm.co m/company/ product- security/bull etins/august- 2021-bulletin	H-QUA-QCA9- 170921/982
qca9988	L			L	
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	08-Sep-21	10	Possible buffer overflow due to improper validation of device types during P2P search in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables,	https://www. qualcomm.co m/company/ product- security/bull etins/august- 2021-bulletin	H-QUA-QCA9- 170921/983

CVSS Scoring Scale	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10
Page 353 of 1474										

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID			
			Snapdragon Wired Infrastructure and Networking					
			CVE ID : CVE-2021-1972					
qca9990								
Out-of- bounds Read	08-Sep-21	3.6	Buffer over read could occur due to incorrect check of buffer size while flashing emmc devices in Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking	https://www. qualcomm.co m/company/ product- security/bull etins/august- 2021-bulletin	H-QUA-QCA9- 170921/984			
			CVE ID : CVE-2021-1928					
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	08-Sep-21	10	Possible buffer overflow due to improper validation of device types during P2P search in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Woice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking CVE ID : CVE-2021-1972	https://www. qualcomm.co m/company/ product- security/bull etins/august- 2021-bulletin	H-QUA-QCA9- 170921/985			
qca9992								
Out-of- bounds Read	08-Sep-21	3.6	Buffer over read could occur due to incorrect check of buffer size while flashing emmc devices in Snapdragon	https://www. qualcomm.co m/company/ product-	H-QUA-QCA9- 170921/986			
CVSS Scoring Sc	ale 0-1	1-2	2-3 3-4 4-5 5-6 Page 354 of 1474	6-7 7-8	8-9 9-10			

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking CVE ID : CVE-2021-1928	security/bull etins/august- 2021-bulletin	
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	08-Sep-21	10	Possible buffer overflow due to improper validation of device types during P2P search in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Industrial IOT, Snapdragon Woile, Snapdragon Woice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking CVE ID : CVE-2021-1972	https://www. qualcomm.co m/company/ product- security/bull etins/august- 2021-bulletin	H-QUA-QCA9- 170921/987
qca9994					L
Out-of-		3.6	Buffer over read could occur due to incorrect check of buffer size while flashing emmc devices in Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking CVE ID : CVE-2021-1928	https://www. qualcomm.co m/company/ product- security/bull etins/august- 2021-bulletin	H-QUA-QCA9- 170921/988
		1-2	2-3 3-4 4-5 5-6	6-7 7-8	8-9 9-10

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID					
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	08-Sep-21	10	Possible buffer overflow due to improper validation of device types during P2P search in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Woice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking CVE ID : CVE-2021-1972	https://www. qualcomm.co m/company/ product- security/bull etins/august- 2021-bulletin	H-QUA-QCA9- 170921/989					
qcm2290	qcm2290									
Exposure of Resource to Wrong Sphere	08-Sep-21	2.1	Child process can leak information from parent process due to numeric pids are getting compared and these pid can be reused in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables CVE ID : CVE-2021-1904	https://www. qualcomm.co m/company/ product- security/bull etins/august- 2021-bulletin	H-QUA-QCM2- 170921/990					
Incorrect Type Conversion or Cast	08-Sep-21	4.6	Incorrect pointer argument passed to trusted application TA could result in un- intended memory operations in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Industrial IOT	https://www. qualcomm.co m/company/ product- security/bull etins/august- 2021-bulletin	H-QUA-QCM2- 170921/991					

1-2

2-3

0-1

4-5

5-6

6-7

7-8

8-9

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2021-1923		
Exposure of Resource to Wrong Sphere	08-Sep-21	2.1	Lack of strict validation of bootmode can lead to information disclosure in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wearables CVE ID : CVE-2021-1929	https://www. qualcomm.co m/company/ product- security/bull etins/august- 2021-bulletin	H-QUA-QCM2- 170921/992
			Possible out of bounds read		
Improper Restriction of Operations within the Bounds of a Memory Buffer	08-Sep-21	3.6	due to incorrect validation of incoming buffer length in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile CVE ID : CVE-2021-1930	https://www. qualcomm.co m/company/ product- security/bull etins/august- 2021-bulletin	H-QUA-QCM2- 170921/993
			Possible buffer overflow due		
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	08-Sep-21	10	to improper validation of device types during P2P search in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Woice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking CVE ID : CVE-2021-1972	https://www. qualcomm.co m/company/ product- security/bull etins/august- 2021-bulletin	H-QUA-QCM2- 170921/994
qcm4290					
CVSS Scoring Sc	ale 0-1	1-2	2-3 3-4 4-5 5-6	6-7 7-8	8-9 9-10
			Page 357 of 1474		

Exposure of Resource to Wrong Sphere08-Sep-212.1Child process can leak information from parent process due to numeric pids are getting compared and these pid can be reused in Snapdragon Compute, Snapdragon Consoumer 107, Snapdragon Outsurial 107, Snapdragon Nobile, Snapdragon Nobile, Snapdragon Nobile, Snapdragon Outsurial 107, Snapdragon Nobile, Snapdragon Note & Music, Snapdragon Note, Snapdragon Consumer 107, Snapdragon Consumer 107, Snapdragon Industrial 107	Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Loop with Unreachable Exit Condition ('Infinite Loop')88-Sep-215condition may occur due to improper handling of unsupported input in Snapdragon Compute, Snapdragon Consumer 107, Snapdragon Industrial 107, Snapdragon Compute, Snapdragon Compute, Snapdragon Compute, Snapdragon Compute, Snapdragon Consumer 107, Snapdragon Industrial 107, Snapdragon Indust	Resource to Wrong	08-Sep-21	2.1	information from parent process due to numeric pids are getting compared and these pid can be reused in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wearables	qualcomm.co m/company/ product- security/bull etins/august-	
Out-of- bounds08-Sep-2110due to lack of check for negative indices values when processing user provided input in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragonhttps://www. qualcomm.co m/company/ product- security/bull etins/august- 2021-bulletinH-QUA-QCM4- 170921/997	Unreachable Exit Condition ('Infinite	08-Sep-21	5	condition may occur due to improper handling of unsupported input in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Voice & Music, Snapdragon Wearables	qualcomm.co m/company/ product- security/bull etins/august-	e e
	bounds	08-Sep-21	10	due to lack of check for negative indices values when processing user provided input in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Voice & Music, Snapdragon	qualcomm.co m/company/ product- security/bull etins/august-	• •

Page 358 of 1474

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2021-1916		
Integer Underflow (Wrap or Wraparoun d)	08-Sep-21	10	Integer underflow can occur when the RTCP length is lesser than than the actual blocks present in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Voice & Music, Snapdragon Wearables CVE ID : CVE-2021-1919	https://www. qualcomm.co m/company/ product- security/bull etins/august- 2021-bulletin	H-QUA-QCM4- 170921/998
Integer Underflow (Wrap or Wraparoun d)	08-Sep-21	10	Integer underflow can occur due to improper handling of incoming RTCP packets in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Voice & Music, Snapdragon Wearables CVE ID : CVE-2021-1920	https://www. qualcomm.co m/company/ product- security/bull etins/august- 2021-bulletin	H-QUA-QCM4- 170921/999
Incorrect Type Conversion or Cast	08-Sep-21	4.6	Incorrect pointer argument passed to trusted application TA could result in un- intended memory operations in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Industrial IOT CVE ID : CVE-2021-1923	https://www. qualcomm.co m/company/ product- security/bull etins/august- 2021-bulletin	H-QUA-QCM4- 170921/1000
Exposure of Resource to Wrong Sphere CVSS Scoring Sc	08-Sep-21 ale 0-1	2.1	Lack of strict validation of bootmode can lead to information disclosure in Snapdragon Auto, 2-3 3-4 4-5 5-6	https://www. qualcomm.co m/company/ product-	H-QUA-QCM4- 170921/1001 8-9 9-10

Page 359 of 1474

Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID	
		Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wearables	security/bull etins/august- 2021-bulletin		
		CVE ID : CVE-2021-1929			
08-Sep-21	3.6	Possible out of bounds read due to incorrect validation of incoming buffer length in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile CVE ID : CVE-2021-1930	https://www. qualcomm.co m/company/ product- security/bull etins/august- 2021-bulletin	H-QUA-QCM4- 170921/1002	
08-Sep-21	10	Possible buffer overflow due to improper validation of device types during P2P search in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Woice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking CVE ID : CVE-2021-1972	https://www. qualcomm.co m/company/ product- security/bull etins/august- 2021-bulletin	H-QUA-QCM4- 170921/1003	
qcm6125					
08-Sep-21	2.1	Child process can leak information from parent process due to numeric pids are getting compared and these pid can be reused in	https://www. qualcomm.co m/company/ product- security/bull	H-QUA-QCM6- 170921/1004	
	08-Sep-21	 Non-state Non-state	outout10Snapdragon Compute, Snapdragon Consumer IOT, Snapdragon Mobile, Snapdragon Mobile, Snapdragon Wearables10CVE ID: CVE-2021-192910Possible out of bounds read due to incorrect validation of incoming buffer length in Snapdragon Auto,08-Sep-213.6Snapdragon Consumer IOT, Snapdragon Auto,08-Sep-213.6Fossible out of bounds read due to incorrect validation of incoming buffer length in Snapdragon Compute, Snapdragon Consumer IOT, Snapdragon Consumer IOT, Snapdragon Mobile08-Sep-211.6Fossible buffer overflow due to improper validation of device types during P2P search in Snapdragon Auto, Snapdragon Consumer IOT, Snapdragon Mobile, Snapdragon Mobile, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking08-Sep-21I.0Snapdragon Wired Infrastructure and Networking08-Sep-21I.0Child process can leak information from parent process due to numeric pids	108-Sep-211108 Snapdragon Consumer IOT, Snapdragon Mobile, Snapdragon Mobile, Snapdragon Mobile, Snapdragon Mobile, Snapdragon Wearablessecurity/bull etins/august- 2021-bulletin08-Sep-2113.6Possible out of bounds read due to incorrect validation of incoming buffer length in Snapdragon Consumer IOT, Snapdragon Consumer IOT, Snapdragon Compute, Snapdragon Mobilehttps://www. qualcomm.co m/company/ product- security/bull etins/august- 2021-bulletin08-Sep-211108Possible buffer overflow due to improper validation of device types during P2P search in Snapdragon Consumer IOT, Snapdragon Consumer IOT, 	

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables CVE ID : CVE-2021-1904	etins/august- 2021-bulletin	
Loop with Unreachable Exit Condition ('Infinite Loop')	08-Sep-21	5	Loop with unreachable exit condition may occur due to improper handling of unsupported input in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Voice & Music, Snapdragon Wearables CVE ID : CVE-2021-1914	https://www. qualcomm.co m/company/ product- security/bull etins/august- 2021-bulletin	H-QUA-QCM6- 170921/1005
Out-of- bounds Write	08-Sep-21	10	Possible buffer underflow due to lack of check for negative indices values when processing user provided input in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Voice & Music, Snapdragon Wearables CVE ID : CVE-2021-1916	https://www. qualcomm.co m/company/ product- security/bull etins/august- 2021-bulletin	H-QUA-QCM6- 170921/1006
Integer Underflow (Wrap or	08-Sep-21	10	Integer underflow can occur when the RTCP length is lesser than than the actual	https://www. qualcomm.co m/company/	H-QUA-QCM6- 170921/1007

CVSS Scoring Scale	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10
Page 361 of 1/7/										

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Wraparoun d)			blocks present in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Voice & Music, Snapdragon Wearables CVE ID : CVE-2021-1919	product- security/bull etins/august- 2021-bulletin	
Integer Underflow (Wrap or Wraparoun d)	08-Sep-21	10	Integer underflow can occur due to improper handling of incoming RTCP packets in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Voice & Music, Snapdragon Wearables CVE ID : CVE-2021-1920	https://www. qualcomm.co m/company/ product- security/bull etins/august- 2021-bulletin	H-QUA-QCM6- 170921/1008
Exposure of Resource to Wrong Sphere	08-Sep-21	2.1	Lack of strict validation of bootmode can lead to information disclosure in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wearables CVE ID : CVE-2021-1929	https://www. qualcomm.co m/company/ product- security/bull etins/august- 2021-bulletin	H-QUA-QCM6- 170921/1009
Improper Restriction of Operations within the Bounds of a	08-Sep-21	3.6	Possible out of bounds read due to incorrect validation of incoming buffer length in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity,	https://www. qualcomm.co m/company/ product- security/bull etins/august-	H-QUA-QCM6- 170921/1010

0-1

1-2

4-5

6-7

5-6

7-8

8-9

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Memory Buffer			Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile	2021-bulletin	
			CVE ID : CVE-2021-1930		
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	08-Sep-21	10	Possible buffer overflow due to improper validation of device types during P2P search in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Woice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking	https://www. qualcomm.co m/company/ product- security/bull etins/august- 2021-bulletin	H-QUA-QCM6- 170921/1011
2040			CVE ID : CVE-2021-1972		
qcn3018					
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	08-Sep-21	10	Possible buffer overflow due to improper validation of device types during P2P search in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Woice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking CVE ID : CVE-2021-1972	https://www. qualcomm.co m/company/ product- security/bull etins/august- 2021-bulletin	H-QUA-QCN3- 170921/1012
qcn5021					
Out-of- bounds	08-Sep-21	3.6	Buffer over read could occur due to incorrect check of	https://www. qualcomm.co	H-QUA-QCN5-
CVSS Scoring Sc	ale 0-1	1-2	2-3 3-4 4-5 5-6 Page 363 of 1474	6-7 7-8	8-9 9-10

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Read			buffer size while flashing emmc devices in Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking CVE ID : CVE-2021-1928	m/company/ product- security/bull etins/august- 2021-bulletin	170921/1013
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	08-Sep-21	10	Possible buffer overflow due to improper validation of device types during P2P search in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Woice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking CVE ID : CVE-2021-1972	https://www. qualcomm.co m/company/ product- security/bull etins/august- 2021-bulletin	H-QUA-QCN5- 170921/1014
qcn5022					
Out-of- bounds Read	08-Sep-21	3.6	Buffer over read could occur due to incorrect check of buffer size while flashing emmc devices in Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and	https://www. qualcomm.co m/company/ product- security/bull etins/august- 2021-bulletin	H-QUA-QCN5- 170921/1015

CVSS Scoring Scale	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10
Page 364 of 1474										

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Networking CVE ID : CVE-2021-1928		
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	08-Sep-21	10	Possible buffer overflow due to improper validation of device types during P2P search in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Woice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking CVE ID : CVE-2021-1972	https://www. qualcomm.co m/company/ product- security/bull etins/august- 2021-bulletin	H-QUA-QCN5- 170921/1016
qcn5024					
Out-of- bounds Read	08-Sep-21	3.6	Buffer over read could occur due to incorrect check of buffer size while flashing emmc devices in Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking CVE ID : CVE-2021-1928	https://www. qualcomm.co m/company/ product- security/bull etins/august- 2021-bulletin	H-QUA-QCN5- 170921/1017
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	08-Sep-21	10	Possible buffer overflow due to improper validation of device types during P2P search in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT,	https://www. qualcomm.co m/company/ product- security/bull etins/august- 2021-bulletin	H-QUA-QCN5- 170921/1018
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 & CVE ID	Patch	NCIIPC ID
			Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking CVE ID : CVE-2021-1972		
qcn5052					
Out-of- bounds Read	08-Sep-21	3.6	Buffer over read could occur due to incorrect check of buffer size while flashing emmc devices in Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking CVE ID : CVE-2021-1928	https://www. qualcomm.co m/company/ product- security/bull etins/august- 2021-bulletin	H-QUA-QCN5- 170921/1019
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	08-Sep-21	10	Possible buffer overflow due to improper validation of device types during P2P search in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Woice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking CVE ID : CVE-2021-1972	https://www. qualcomm.co m/company/ product- security/bull etins/august- 2021-bulletin	H-QUA-QCN5- 170921/1020
qcn5054	I			I	I
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 & CVE ID	Patch	NCIIPC ID
Out-of- bounds Read	08-Sep-21	3.6	Buffer over read could occur due to incorrect check of buffer size while flashing emmc devices in Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking CVE ID : CVE-2021-1928	https://www. qualcomm.co m/company/ product- security/bull etins/august- 2021-bulletin	H-QUA-QCN5- 170921/1021
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	08-Sep-21	10	Possible buffer overflow due to improper validation of device types during P2P search in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Industrial IOT, Snapdragon Woice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking CVE ID : CVE-2021-1972	https://www. qualcomm.co m/company/ product- security/bull etins/august- 2021-bulletin	H-QUA-QCN5- 170921/1022
qcn5064					
Out-of- bounds Read	08-Sep-21	3.6	Buffer over read could occur due to incorrect check of buffer size while flashing emmc devices in Snapdragon Connectivity, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon	https://www. qualcomm.co m/company/ product- security/bull etins/august- 2021-bulletin	H-QUA-QCN5- 170921/1023

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Wired Infrastructure and Networking		
			CVE ID : CVE-2021-1928		
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	08-Sep-21	10	Possible buffer overflow due to improper validation of device types during P2P search in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Woice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking	https://www. qualcomm.co m/company/ product- security/bull etins/august- 2021-bulletin	H-QUA-QCN5- 170921/1024
F404			CVE ID : CVE-2021-1972		
qcn5121				ſ	Γ
Out-of- bounds Read	08-Sep-21	3.6	Buffer over read could occur due to incorrect check of buffer size while flashing emmc devices in Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking CVE ID : CVE-2021-1928	https://www. qualcomm.co m/company/ product- security/bull etins/august- 2021-bulletin	H-QUA-QCN5- 170921/1025
Buffer Copy			Possible buffer overflow due	https://www.	
without Checking Size of Input ('Classic Buffer	08-Sep-21	10	to improper validation of device types during P2P search in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity,	qualcomm.co m/company/ product- security/bull etins/august-	H-QUA-QCN5- 170921/1026
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 & CVE ID	Patch	NCIIPC ID
Overflow')			Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking CVE ID : CVE-2021-1972	2021-bulletin	
qcn5122				I	L
Out-of- bounds Read	08-Sep-21	3.6	Buffer over read could occur due to incorrect check of buffer size while flashing emmc devices in Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking	https://www. qualcomm.co m/company/ product- security/bull etins/august- 2021-bulletin	H-QUA-QCN5- 170921/1027
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	08-Sep-21 ale 0-1	10	CVE ID : CVE-2021-1928Possible buffer overflow dueto improper validation ofdevice types during P2Psearch in Snapdragon Auto,Snapdragon Compute,Snapdragon Compute,Snapdragon Connectivity,Snapdragon Consumer IOT,Snapdragon Consumer IOT,Snapdragon Mobile,Snapdragon Mobile,Snapdragon Wearables,Snapdragon WiredInfrastructure andNetworkingCVE ID : CVE-2021-1972	https://www. qualcomm.co m/company/ product- security/bull etins/august- 2021-bulletin	H-QUA-QCN5- 170921/1028

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
qcn5124					
Out-of- bounds Read	08-Sep-21	3.6	Buffer over read could occur due to incorrect check of buffer size while flashing emmc devices in Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking CVE ID : CVE-2021-1928	https://www. qualcomm.co m/company/ product- security/bull etins/august- 2021-bulletin	H-QUA-QCN5- 170921/1029
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	08-Sep-21	10	Possible buffer overflow due to improper validation of device types during P2P search in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Woice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking CVE ID : CVE-2021-1972	https://www. qualcomm.co m/company/ product- security/bull etins/august- 2021-bulletin	H-QUA-QCN5- 170921/1030
qcn5152				I	
Out-of- bounds Read	08-Sep-21	3.6	Buffer over read could occur due to incorrect check of buffer size while flashing emmc devices in Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice &	https://www. qualcomm.co m/company/ product- security/bull etins/august- 2021-bulletin	H-QUA-QCN5- 170921/1031

0-1

1-2

5-6

6-7

7-8

8-9

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking		
			CVE ID : CVE-2021-1928		
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	08-Sep-21	10	Possible buffer overflow due to improper validation of device types during P2P search in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Woice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking CVE ID : CVE-2021-1972	https://www. qualcomm.co m/company/ product- security/bull etins/august- 2021-bulletin	H-QUA-QCN5- 170921/1032
qcn5154					
Out-of- bounds Read	08-Sep-21	3.6	Buffer over read could occur due to incorrect check of buffer size while flashing emmc devices in Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking CVE ID : CVE-2021-1928	https://www. qualcomm.co m/company/ product- security/bull etins/august- 2021-bulletin	H-QUA-QCN5- 170921/1033
Buffer Copy without Checking Size of Input	08-Sep-21	10	Possible buffer overflow due to improper validation of device types during P2P search in Snapdragon Auto,	https://www. qualcomm.co m/company/ product-	H-QUA-QCN5- 170921/1034
CVSS Scoring Sc	ale 0-1	1-2	2-3 3-4 4-5 5-6	6-7 7-8	8-9 9-10

Page 371 of 1474

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
('Classic Buffer Overflow')			Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking CVE ID : CVE-2021-1972	security/bull etins/august- 2021-bulletin	
qcn5164					
Out-of- bounds Read	08-Sep-21	3.6	Buffer over read could occur due to incorrect check of buffer size while flashing emmc devices in Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking CVE ID : CVE-2021-1928	https://www. qualcomm.co m/company/ product- security/bull etins/august- 2021-bulletin	H-QUA-QCN5- 170921/1035
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	08-Sep-21	10	Possible buffer overflow due to improper validation of device types during P2P search in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wired Snapdragon Wired Infrastructure and	https://www. qualcomm.co m/company/ product- security/bull etins/august- 2021-bulletin	H-QUA-QCN5- 170921/1036

CVSS Scoring Scale	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10
			P	age 372 c	of 1474					

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Networking		
			CVE ID : CVE-2021-1972		
qcn5500					
Out-of- bounds Read	08-Sep-21	3.6	Buffer over read could occur due to incorrect check of buffer size while flashing emmc devices in Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking CVE ID : CVE-2021-1928	https://www. qualcomm.co m/company/ product- security/bull etins/august- 2021-bulletin	H-QUA-QCN5- 170921/1037
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	08-Sep-21	10	Possible buffer overflow due to improper validation of device types during P2P search in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Woice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking CVE ID : CVE-2021-1972	https://www. qualcomm.co m/company/ product- security/bull etins/august- 2021-bulletin	H-QUA-QCN5- 170921/1038
qcn5502					<u> </u>
Out-of- bounds Read	08-Sep-21	3.6	Buffer over read could occur due to incorrect check of buffer size while flashing emmc devices in Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon	https://www. qualcomm.co m/company/ product- security/bull etins/august-	H-QUA-QCN5- 170921/1039
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 & CVE ID	Patch	NCIIPC ID
			Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking	2021-bulletin	
			CVE ID : CVE-2021-1928		
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	08-Sep-21	10	Possible buffer overflow due to improper validation of device types during P2P search in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Woice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking CVE ID : CVE-2021-1972	https://www. qualcomm.co m/company/ product- security/bull etins/august- 2021-bulletin	H-QUA-QCN5- 170921/1040
qcn5550					
Out-of- bounds Read	08-Sep-21	3.6	Buffer over read could occur due to incorrect check of buffer size while flashing emmc devices in Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking CVE ID : CVE-2021-1928	https://www. qualcomm.co m/company/ product- security/bull etins/august- 2021-bulletin	H-QUA-QCN5- 170921/1041
Buffer Copy without	08-Sep-21	10	Possible buffer overflow due to improper validation of	https://www. qualcomm.co	H-QUA-QCN5- 170921/1042

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Checking Size of Input ('Classic Buffer Overflow')			device types during P2P search in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Woice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking CVE ID : CVE-2021-1972	m/company/ product- security/bull etins/august- 2021-bulletin	
qcn6023					
Out-of- bounds Read	08-Sep-21	3.6	Buffer over read could occur due to incorrect check of buffer size while flashing emmc devices in Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking	https://www. qualcomm.co m/company/ product- security/bull etins/august- 2021-bulletin	H-QUA-QCN6- 170921/1043
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	08-Sep-21	10	CVE ID : CVE-2021-1928 Possible buffer overflow due to improper validation of device types during P2P search in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Woice & Music, Snapdragon Wearables, Snapdragon Wired	https://www. qualcomm.co m/company/ product- security/bull etins/august- 2021-bulletin	H-QUA-QCN6- 170921/1044

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID			
			Infrastructure and Networking					
			6					
			CVE ID : CVE-2021-1972					
qcn6024								
Out-of- bounds Read	08-Sep-21	3.6	Buffer over read could occur due to incorrect check of buffer size while flashing emmc devices in Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking CVE ID : CVE-2021-1928	https://www. qualcomm.co m/company/ product- security/bull etins/august- 2021-bulletin	H-QUA-QCN6- 170921/1045			
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	08-Sep-21	10	Possible buffer overflow due to improper validation of device types during P2P search in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Woice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking CVE ID : CVE-2021-1972	https://www. qualcomm.co m/company/ product- security/bull etins/august- 2021-bulletin	H-QUA-QCN6- 170921/1046			
qcn6122	qcn6122							
Buffer Copy without Checking Size of Input ('Classic	08-Sep-21	10	Possible buffer overflow due to improper validation of device types during P2P search in Snapdragon Auto, Snapdragon Compute,	https://www. qualcomm.co m/company/ product- security/bull	H-QUA-QCN6- 170921/1047			
CVSS Scoring Sc	ale 0-1	1-2	2-3 3-4 4-5 5-6 Page 376 of 1474	6-7 7-8	8-9 9-10			

Page 376 of 1474

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Buffer Overflow')			Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking CVE ID : CVE-2021-1972	etins/august- 2021-bulletin	
qcn9000					
Out-of- bounds Read	08-Sep-21	3.6	Buffer over read could occur due to incorrect check of buffer size while flashing emmc devices in Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking CVE ID : CVE-2021-1928	https://www. qualcomm.co m/company/ product- security/bull etins/august- 2021-bulletin	H-QUA-QCN9- 170921/1048
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	08-Sep-21	10	Possible buffer overflow due to improper validation of device types during P2P search in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Woice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking	https://www. qualcomm.co m/company/ product- security/bull etins/august- 2021-bulletin	H-QUA-QCN9- 170921/1049

CVSS Scoring Scale	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10
			D	277 0	f 1/7/					

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2021-1972		
qcn9012					
Out-of- bounds Read	08-Sep-21	3.6	Buffer over read could occur due to incorrect check of buffer size while flashing emmc devices in Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking	https://www. qualcomm.co m/company/ product- security/bull etins/august- 2021-bulletin	H-QUA-QCN9- 170921/1050
			CVE ID : CVE-2021-1928		
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	08-Sep-21	10	Possible buffer overflow due to improper validation of device types during P2P search in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Industrial IOT, Snapdragon Woile, Snapdragon Woice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking CVE ID : CVE-2021-1972	https://www. qualcomm.co m/company/ product- security/bull etins/august- 2021-bulletin	H-QUA-QCN9- 170921/1051
qcn9022					
Out-of- bounds Read	08-Sep-21	3.6	Buffer over read could occur due to incorrect check of buffer size while flashing emmc devices in Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon	https://www. qualcomm.co m/company/ product- security/bull etins/august- 2021-bulletin	H-QUA-QCN9- 170921/1052
CVSS Scoring Sc	ale 0-1	1-2	2-3 3-4 4-5 5-6 Page 378 of 1474	6-7 7-8	8-9 9-10

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Mobile, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking		
			CVE ID : CVE-2021-1928		
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	08-Sep-21	10	Possible buffer overflow due to improper validation of device types during P2P search in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Woice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking CVE ID : CVE-2021-1972	https://www. qualcomm.co m/company/ product- security/bull etins/august- 2021-bulletin	H-QUA-QCN9- 170921/1053
qcn9024					
Out-of- bounds Read	08-Sep-21	3.6	Buffer over read could occur due to incorrect check of buffer size while flashing emmc devices in Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking CVE ID : CVE-2021-1928	https://www. qualcomm.co m/company/ product- security/bull etins/august- 2021-bulletin	H-QUA-QCN9- 170921/1054
Buffer Copy without Checking	08-Sep-21	10	Possible buffer overflow due to improper validation of device types during P2P	https://www. qualcomm.co m/company/	H-QUA-QCN9- 170921/1055
CVSS Scoring Sc	ale 0-1	1-2	2-3 3-4 4-5 5-6	6-7 7-8	8-9 9-10

Page 379 of 1474

Size of Input ('Classic Buffer Overflow')			search in Snapdragon Auto, Snapdragon Compute,	product-	
			Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking CVE ID : CVE-2021-1972	security/bull etins/august- 2021-bulletin	
qcn9070					
Out-of- bounds Read	08-Sep-21	3.6	Buffer over read could occur due to incorrect check of buffer size while flashing emmc devices in Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking CVE ID : CVE-2021-1928	https://www. qualcomm.co m/company/ product- security/bull etins/august- 2021-bulletin	H-QUA-QCN9- 170921/1056
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	08-Sep-21	10	Possible buffer overflow due to improper validation of device types during P2P search in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Woice & Music, Snapdragon Wired Infrastructure and	https://www. qualcomm.co m/company/ product- security/bull etins/august- 2021-bulletin	H-QUA-QCN9- 170921/1057

Page 380 of 1474

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID	
			Networking			
			CVE ID : CVE-2021-1972			
qcn9072						
Out-of- bounds Read	ınds 08-Sep-21 <mark>3.6</mark>		Buffer over read could occur due to incorrect check of buffer size while flashing emmc devices in Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking CVE ID : CVE-2021-1928	https://www. qualcomm.co m/company/ product- security/bull etins/august- 2021-bulletin	H-QUA-QCN9- 170921/1058	
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	08-Sep-21	10	Possible buffer overflow due to improper validation of device types during P2P search in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Woice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking CVE ID : CVE-2021-1972	https://www. qualcomm.co m/company/ product- security/bull etins/august- 2021-bulletin	H-QUA-QCN9- 170921/1059	
qcn9074						
Out-of- bounds 08-Sep-21		3.6	Buffer over read could occur due to incorrect check of buffer size while flashing emmc devices in Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon	https://www. qualcomm.co m/company/ product- security/bull etins/august-	H-QUA-QCN9- 170921/1060	
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 & CVE ID	Patch	NCIIPC ID
			Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking	2021-bulletin	
			CVE ID : CVE-2021-1928		
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	08-Sep-21	10	Possible buffer overflow due to improper validation of device types during P2P search in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Woice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking CVE ID : CVE-2021-1972	https://www. qualcomm.co m/company/ product- security/bull etins/august- 2021-bulletin	H-QUA-QCN9- 170921/1061
qcn9100					
Out-of- bounds Read	08-Sep-21	3.6	Buffer over read could occur due to incorrect check of buffer size while flashing emmc devices in Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking CVE ID : CVE-2021-1928	https://www. qualcomm.co m/company/ product- security/bull etins/august- 2021-bulletin	H-QUA-QCN9- 170921/1062
Buffer Copy without	08-Sep-21	10	Possible buffer overflow due to improper validation of	https://www. qualcomm.co	H-QUA-QCN9- 170921/1063

Weakness	Publish Date	CVSS	Descript	on & CVE I	D	Pa	tch	NCII	PC ID
Checking Size of Input ('Classic Buffer Overflow')			device types of search in Sna Snapdragon (Snapdragon (Sna) (Snapdragon (Sna) (Sna	m/com produc securit etins/a 2021-b	ct- y/bull ugust-				
qcs2290			CVEID.CVE	-2021-15					
Exposure of Resource to Wrong Sphere	08-Sep-21	2.1	Child process information f process due t are getting co these pid can Snapdragon f Snapdragon f	https:/ qualcom m/com product securit etins/a 2021-b	ipany/ ct- y/bull iugust-	-	-QCS2- 1/1064		
Incorrect Type Conversion or Cast	08-Sep-21	4.6	Incorrect pointer argument passed to trusted application TA could result in un- intended memory operations in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Industrial IOT CVE ID : CVE-2021-1923			https:/ qualcom m/com produc securit etins/a 2021-b	ipany/ t- y/bull iugust-	-	-QCS2- 1/1065
Exposure of	08-Sep-21	2.1	Lack of strict	https:/	/www.	H-QUA	-QCS2-		
CVSS Scoring Sc	ale 0-1	1-2	2-3 3-4	4-5	5-6	6-7	7-8	8-9	9-10

Page 383 of 1474

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Resource to Wrong Sphere			bootmode can lead to information disclosure in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wearables CVE ID : CVE-2021-1929	qualcomm.co m/company/ product- security/bull etins/august- 2021-bulletin	170921/1066
Improper Restriction of Operations within the Bounds of a Memory Buffer	08-Sep-21	3.6	Possible out of bounds read due to incorrect validation of incoming buffer length in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile CVE ID : CVE-2021-1930	https://www. qualcomm.co m/company/ product- security/bull etins/august- 2021-bulletin	H-QUA-QCS2- 170921/1067
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	08-Sep-21	10	Possible buffer overflow due to improper validation of device types during P2P search in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Woice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking CVE ID : CVE-2021-1972	https://www. qualcomm.co m/company/ product- security/bull etins/august- 2021-bulletin	H-QUA-QCS2- 170921/1068
qcs405				I	I
Exposure of Resource to	08-Sep-21	2.1	Child process can leak information from parent	https://www. qualcomm.co	H-QUA-QCS4- 170921/1069
CVSS Scoring Sc	ale 0-1	1-2	2-3 3-4 4-5 5-6 Page 384 of 1474	6-7 7-8	8-9 9-10

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Wrong Sphere			process due to numeric pids are getting compared and these pid can be reused in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wearables CVE ID : CVE-2021-1904	m/company/ product- security/bull etins/august- 2021-bulletin	
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	08-Sep-21	10	Possible buffer overflow due to improper validation of device types during P2P search in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Industrial IOT, Snapdragon Woile, Snapdragon Woice & Music, Snapdragon Wired Infrastructure and Networking CVE ID : CVE-2021-1972	https://www. qualcomm.co m/company/ product- security/bull etins/august- 2021-bulletin	H-QUA-QCS4- 170921/1070
qcs410					
Exposure of Resource to Wrong Sphere		Child process can leak information from parent process due to numeric pids are getting compared and these pid can be reused in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile,	https://www. qualcomm.co m/company/ product- security/bull etins/august- 2021-bulletin	H-QUA-QCS4- 170921/1071	
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 & CVE ID	Patch	NCIIPC ID
			Snapdragon Voice & Music, Snapdragon Wearables		
			CVE ID : CVE-2021-1904		
Loop with Unreachable Exit Condition ('Infinite Loop')	08-Sep-21	5	Loop with unreachable exit condition may occur due to improper handling of unsupported input in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Voice & Music, Snapdragon Wearables CVE ID : CVE-2021-1914	https://www. qualcomm.co m/company/ product- security/bull etins/august- 2021-bulletin	H-QUA-QCS4- 170921/1072
Out-of- bounds Write	08-Sep-21	 input in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, 		https://www. qualcomm.co m/company/ product- security/bull etins/august- 2021-bulletin	H-QUA-QCS4- 170921/1073
Integer Underflow (Wrap or Wraparoun d)	08-Sep-21	10	CVE ID : CVE-2021-1916 Integer underflow can occur when the RTCP length is lesser than than the actual blocks present in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon	https://www. qualcomm.co m/company/ product- security/bull etins/august- 2021-bulletin	H-QUA-QCS4- 170921/1074

1-2 2-3

0-1

5-6

6-7

7-8

8-9

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID	
			Voice & Music, Snapdragon Wearables			
			CVE ID : CVE-2021-1919			
Integer Underflow (Wrap or Wraparoun d)	08-Sep-21	10	Integer underflow can occur due to improper handling of incoming RTCP packets in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Voice & Music, Snapdragon Wearables	https://www. qualcomm.co m/company/ product- security/bull etins/august- 2021-bulletin	H-QUA-QCS4- 170921/1075	
			CVE ID : CVE-2021-1920			
Improper Restriction of Operations within the Bounds of a Memory Buffer	08-Sep-21 and the set of the set		due to incorrect validation of incoming buffer length in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT,	https://www. qualcomm.co m/company/ product- security/bull etins/august- 2021-bulletin	H-QUA-QCS4- 170921/1076	
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	08-Sep-21	10	Possible buffer overflow due to improper validation of device types during P2P search in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Woice & Music, Snapdragon Wired Infrastructure and	https://www. qualcomm.co m/company/ product- security/bull etins/august- 2021-bulletin	H-QUA-QCS4- 170921/1077	

0-1

1-2

2-3 3-4 4-5

5-6

6-7

7-8

8-9

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID	
			Networking			
			CVE ID : CVE-2021-1972			
qcs4290						
Exposure of Resource to Wrong Sphere	08-Sep-21	2.1	Child process can leak information from parent process due to numeric pids are getting compared and these pid can be reused in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, 		H-QUA-QCS4- 170921/1078	
Loop with Unreachable Exit Condition ('Infinite Loop')	08-Sep-21	5	Loop with unreachable exit condition may occur due to improper handling of unsupported input in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Voice & Music, Snapdragon Wearables CVE ID : CVE-2021-1914	https://www. qualcomm.co m/company/ product- security/bull etins/august- 2021-bulletin	H-QUA-QCS4- 170921/1079	
Out-of- bounds Write	08-Sep-21 10		Possible buffer underflow due to lack of check for negative indices values when processing user provided input in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT,	https://www. qualcomm.co m/company/ product- security/bull etins/august- 2021-bulletin	H-QUA-QCS4- 170921/1080	
CVSS Scoring Sc	ale 0-1	1-2	2-3 3-4 4-5 5-6	6-7 7-8	8-9 9-10	

Page 388 of 1474

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Voice & Music, Snapdragon Wearables		
			CVE ID : CVE-2021-1916		
Integer Underflow (Wrap or Wraparoun d)	08-Sep-21	10	Integer underflow can occur when the RTCP length is lesser than than the actual blocks present in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Voice & Music, Snapdragon Wearables CVE ID : CVE-2021-1919	https://www. qualcomm.co m/company/ product- security/bull etins/august- 2021-bulletin	H-QUA-QCS4- 170921/1081
Integer Underflow (Wrap or Wraparoun d)	08-Sep-21	10	Integer underflow can occur due to improper handling of incoming RTCP packets in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Voice & Music, Snapdragon Wearables CVE ID : CVE-2021-1920	https://www. qualcomm.co m/company/ product- security/bull etins/august- 2021-bulletin	H-QUA-QCS4- 170921/1082
Incorrect Type Conversion or Cast	08-Sep-21	4.6	Incorrect pointer argument passed to trusted application TA could result in un- intended memory operations in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Industrial IOT CVE ID : CVE-2021-1923	https://www. qualcomm.co m/company/ product- security/bull etins/august- 2021-bulletin	H-QUA-QCS4- 170921/1083
CVSS Scoring Sc	ale 0-1	1-2	2-3 3-4 4-5 5-6 Page 389 of 1474	6-7 7-8	8-9 9-10

Page 389 of 1474

Exposure of Resource to Wrong Sphere08-Sep-21Lack of strict validation of bootmode can lead to information disclosure in Snapdragon Auto, Snapdragon Consumer 10T, Snapdragon Mobilehttps://www. qualcomm.co m/company/ product- security/bull etins/august- 2021-bulletinH-QUA-QCS4- 170921/1084Buffer Copy without (Classic Buffer08-Sep-213.6Possible out of bounds read due to incorrect validation of incoming buffer length in Snapdragon Consumer 10T, Snapdragon Mobilehttps://www. qualcomm.co m/company/ product- security/bull etins/august- 2021-bulletinBuffer Copy without (Classic Buffer08-Sep-213.6Possible buffer overflow due to impoper validation of device types during P2P search in Snapdragon Consumer 10T, Snapdragon Nobile, Snapdragon Nobile, Snapdragon Nobile, Snapdragon Voice & Music, Snapdragon Nobile, Snapdragon Wearables, Snapdragon Wearables, Snapdragon Wired Infastructure and Networking CV	Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Improper Restriction of Operations within the Bounds of a Memory Buffer08-Sep-213.6due to incorrect validation of incoming buffer length in Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobilehttps://www. qualcomm.co m/company/ product- security/bull etins/august- 2021-bulletinH-QUA-QCS4- 170921/1085Buffer08-Sep-213.6Possible buffer overflow due to improper validation of device types during P2P search in Snapdragon Consumer IOT, Snapdragon Mobile, Snapdragon Wired Infrastructure and NetworkingH-QUA-QCS4- 170921/1086tresttresttresttresttresttresttrestges603trestt	Resource to Wrong	08-Sep-21	2.1	bootmode can lead to information disclosure in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wearables	qualcomm.co m/company/ product- security/bull etins/august-	
Buffer Copy without Checking Size of Input ('Classic Dverflow')to improper validation of device types during P2P search in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networkinghttps://www. qualcomm.co m/company/ product- security/bull etins/august- 2021-bulletinH-QUA-QCS4- 170921/1086gres603CVE ID : CVE-2021-1972Ittps://www. Buffer Overflow')H-QUA-QCS4- 170921/1086buffer Overflow')08-Sep-212.1Child process can leakhttps://www. buffer BufferH-QUA-QCS4- 170921/1086buffer Overflow')08-Sep-212.1Child process can leakhttps://www. bufferH-QUA-QCS4- 170921/1086buffer Overflow')08-Sep-212.1Child process can leakhttps://www. bufferH-QUA-QCS4- 170921/1086buffer Overflow')08-Sep-212.1Child process can leakhttps://www. bufferH-QUA-QCS4- 	Restriction of Operations within the Bounds of a Memory	08-Sep-21	3.6	due to incorrect validation of incoming buffer length in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile	qualcomm.co m/company/ product- security/bull etins/august-	
Exposure of 08-Sep-21 2.1 Child process can leak https://www. H-QUA-QCS6-	without Checking Size of Input ('Classic Buffer	08-Sep-21	10	to improper validation of device types during P2P search in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Woice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking	qualcomm.co m/company/ product- security/bull etins/august-	
	qcs603					<u> </u>
	Exposure of	08-Sep-21	2.1	Child process can leak	https://www.	H-QUA-QCS6-

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Resource to Wrong Sphere			information from parent process due to numeric pids are getting compared and these pid can be reused in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wearables CVE ID : CVE-2021-1904	qualcomm.co m/company/ product- security/bull etins/august- 2021-bulletin	170921/1087
Loop with Unreachable Exit Condition ('Infinite Loop')	08-Sep-21	5	Loop with unreachable exit condition may occur due to improper handling of unsupported input in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Voice & Music, Snapdragon Wearables CVE ID : CVE-2021-1914	https://www. qualcomm.co m/company/ product- security/bull etins/august- 2021-bulletin	H-QUA-QCS6- 170921/1088
Out-of- bounds Write	08-Sep-21	10	Possible buffer underflow due to lack of check for negative indices values when processing user provided input in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Voice & Music, Snapdragon Wearables	https://www. qualcomm.co m/company/ product- security/bull etins/august- 2021-bulletin	H-QUA-QCS6- 170921/1089

[CVSS Scoring Scale	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10
	Page 391 of 1/7/										

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2021-1916		
Integer Underflow (Wrap or Wraparoun d)	08-Sep-21	10	Integer underflow can occur when the RTCP length is lesser than than the actual blocks present in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Voice & Music, Snapdragon Wearables CVE ID : CVE-2021-1919	https://www. qualcomm.co m/company/ product- security/bull etins/august- 2021-bulletin	H-QUA-QCS6- 170921/1090
Integer Underflow (Wrap or Wraparoun d)	08-Sep-21	10	Integer underflow can occur due to improper handling of incoming RTCP packets in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Voice & Music, Snapdragon Wearables CVE ID : CVE-2021-1920	https://www. qualcomm.co m/company/ product- security/bull etins/august- 2021-bulletin	H-QUA-QCS6- 170921/1091
Exposure of Resource to Wrong Sphere	08-Sep-21	2.1	Lack of strict validation of bootmode can lead to information disclosure in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wearables CVE ID : CVE-2021-1929	https://www. qualcomm.co m/company/ product- security/bull etins/august- 2021-bulletin	H-QUA-QCS6- 170921/1092
Buffer Copy without	08-Sep-21	10	Possible buffer overflow due to improper validation of	https://www. qualcomm.co	H-QUA-QCS6- 170921/1093

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Checking Size of Input ('Classic Buffer Overflow')			device types during P2P search in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Woice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking CVE ID : CVE-2021-1972	m/company/ product- security/bull etins/august- 2021-bulletin	
qcs605					
Exposure of Resource to Wrong Sphere		2.1	Child process can leak information from parent process due to numeric pids are getting compared and these pid can be reused in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables CVE ID : CVE-2021-1904	https://www. qualcomm.co m/company/ product- security/bull etins/august- 2021-bulletin	H-QUA-QCS6- 170921/1094
Loop with Unreachable Exit Condition ('Infinite Loop') 08-Sep-21 5		Loop with unreachable exit condition may occur due to improper handling of unsupported input in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Voice & Music, Snapdragon	https://www. qualcomm.co m/company/ product- security/bull etins/august- 2021-bulletin	H-QUA-QCS6- 170921/1095	

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID		
			Wearables				
			CVE ID : CVE-2021-1914				
Out-of- bounds Write	08-Sep-21	10	Possible buffer underflow due to lack of check for negative indices values when processing user provided input in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Voice & Music, Snapdragon Wearables	https://www. qualcomm.co m/company/ product- security/bull etins/august- 2021-bulletin	H-QUA-QCS6- 170921/1096		
			CVE ID : CVE-2021-1916				
Integer Underflow (Wrap or Wraparoun d)	08-Sep-21	10	Integer underflow can occur when the RTCP length is lesser than than the actual blocks present in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Voice & Music, Snapdragon Wearables CVE ID : CVE-2021-1919	https://www. qualcomm.co m/company/ product- security/bull etins/august- 2021-bulletin	H-QUA-QCS6- 170921/1097		
Integer Underflow (Wrap or Wraparoun d)	08-Sep-21	10	Integer underflow can occur due to improper handling of incoming RTCP packets in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Voice & Music, Snapdragon Wearables	https://www. qualcomm.co m/company/ product- security/bull etins/august- 2021-bulletin	H-QUA-QCS6- 170921/1098		
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	
			CVE ID : CVE-2021-1920			
Exposure of Resource to Wrong Sphere	08-Sep-21	2.1	Lack of strict validation of bootmode can lead to information disclosure in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wearables CVE ID : CVE-2021-1929	https://www. qualcomm.co m/company/ product- security/bull etins/august- 2021-bulletin	H-QUA-QCS6- 170921/1099	
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	08-Sep-21	10	Possible buffer overflow due to improper validation of device types during P2P search in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Woice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking CVE ID : CVE-2021-1972	https://www. qualcomm.co m/company/ product- security/bull etins/august- 2021-bulletin	H-QUA-QCS6- 170921/1100	
qcs610						
Exposure of Resource to Wrong Sphere	08-Sep-21	2.1	Child process can leak information from parent process due to numeric pids are getting compared and these pid can be reused in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT,	https://www. qualcomm.co m/company/ product- security/bull etins/august- 2021-bulletin	H-QUA-QCS6- 170921/1101	

CVSS Scoring Scale	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10
Page 395 of 1474										

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables CVE ID : CVE-2021-1904		
Loop with Unreachable Exit Condition ('Infinite Loop')	08-Sep-21	5	Loop with unreachable exit condition may occur due to improper handling of unsupported input in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Voice & Music, Snapdragon Wearables	https://www. qualcomm.co m/company/ product- security/bull etins/august- 2021-bulletin	H-QUA-QCS6- 170921/1102
Out-of- bounds Write	08-Sep-21	10	CVE ID : CVE-2021-1914 Possible buffer underflow due to lack of check for negative indices values when processing user provided input in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Voice & Music, Snapdragon Wearables CVE ID : CVE-2021-1916	https://www. qualcomm.co m/company/ product- security/bull etins/august- 2021-bulletin	H-QUA-QCS6- 170921/1103
Integer Underflow (Wrap or Wraparoun d)	08-Sep-21	10	Integer underflow can occur when the RTCP length is lesser than than the actual blocks present in Snapdragon Auto, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT,https://www. qualcomm.co m/company/ product- security/bull etins/august- 2021-bulletin		H-QUA-QCS6- 170921/1104

1-2 2-3

0-1

4-5

5-6

6-7

7-8

8-9

9-10

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Snapdragon IoT, Snapdragon Voice & Music, Snapdragon Wearables		
			CVE ID : CVE-2021-1919		
Integer Underflow (Wrap or Wraparoun d)	08-Sep-21	10	Integer underflow can occur due to improper handling of incoming RTCP packets in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Voice & Music, Snapdragon Wearables CVE ID : CVE-2021-1920	https://www. qualcomm.co m/company/ product- security/bull etins/august- 2021-bulletin	H-QUA-QCS6- 170921/1105
Exposure of Resource to Wrong Sphere	08-Sep-21	2.1	Lack of strict validation of bootmode can lead to information disclosure in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wearables CVE ID : CVE-2021-1929	https://www. qualcomm.co m/company/ product- security/bull etins/august- 2021-bulletin	H-QUA-QCS6- 170921/1106
Improper Restriction of Operations within the Bounds of a Memory Buffer	08-Sep-21	3.6	Possible out of bounds read due to incorrect validation of incoming buffer length in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile CVE ID : CVE-2021-1930	https://www. qualcomm.co m/company/ product- security/bull etins/august- 2021-bulletin	H-QUA-QCS6- 170921/1107

CVSS Scoring Scale	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10
Page 397 of 1474										

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	08-Sep-21	10	Possible buffer overflow due to improper validation of device types during P2P search in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Woice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking CVE ID : CVE-2021-1972	https://www. qualcomm.co m/company/ product- security/bull etins/august- 2021-bulletin	H-QUA-QCS6- 170921/1108
qcs6125					
Exposure of Resource to Wrong Sphere	08-Sep-21	2.1	Child process can leak information from parent process due to numeric pids are getting compared and these pid can be reused in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables CVE ID : CVE-2021-1904	https://www. qualcomm.co m/company/ product- security/bull etins/august- 2021-bulletin	H-QUA-QCS6- 170921/1109
Loop with Unreachable Exit Condition ('Infinite Loop')	08-Sep-21	5	Loop with unreachable exit condition may occur due to improper handling of unsupported input in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT,	https://www. qualcomm.co m/company/ product- security/bull etins/august- 2021-bulletin	H-QUA-QCS6- 170921/1110

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Snapdragon IoT, Snapdragon Voice & Music, Snapdragon Wearables		
			CVE ID : CVE-2021-1914		
Out-of- bounds Write	08-Sep-21	10	Possible buffer underflow due to lack of check for negative indices values when processing user provided input in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Voice & Music, Snapdragon Wearables	https://www. qualcomm.co m/company/ product- security/bull etins/august- 2021-bulletin	H-QUA-QCS6- 170921/1111
Integer	low or 08-Sep-21 10		CVE ID : CVE-2021-1916 Integer underflow can occur when the RTCP length is lesser than than the actual blocks present in Snapdragon Auto, Snapdragon Compute,	https://www. qualcomm.co	
Underflow		Snapdragon Connectivity,		m/company/ product- security/bull etins/august- 2021-bulletin	H-QUA-QCS6- 170921/1112
			CVE ID : CVE-2021-1919		
Integer Underflow (Wrap or Wraparoun d)	08-Sep-21	10	Integer underflow can occur due to improper handling of incoming RTCP packets in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon	https://www. qualcomm.co m/company/ product- security/bull etins/august- 2021-bulletin	H-QUA-QCS6- 170921/1113

1-2

0-1

5-6

6-7

7-8

8-9

		Voice & Music, Snapdragon		
		Wearables CVE ID : CVE-2021-1920		
S-Sep-21	2.1	Lack of strict validation of bootmode can lead to information disclosure in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wearables	https://www. qualcomm.co m/company/ product- security/bull etins/august- 2021-bulletin	H-QUA-QCS6- 170921/1114
S-Sep-21	3.6	due to incorrect validation of incoming buffer length in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile	https://www. qualcomm.co m/company/ product- security/bull etins/august- 2021-bulletin	H-QUA-QCS6- 170921/1115
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')		Possible buffer overflow due to improper validation of device types during P2P search in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Woice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking	https://www. qualcomm.co m/company/ product- security/bull etins/august- 2021-bulletin	H-QUA-QCS6- 170921/1116
	Sep-21	. . Sep-21 3.6 . . Sep-21 10	Sep-21Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Mobile, Snapdragon Mobile, Snapdragon WearablesSep-212.1Snapdragon Consumer IOT, Snapdragon Mobile, Snapdragon WearablesSep-213.6Possible out of bounds read due to incorrect validation of incoming buffer length in Snapdragon Compute, Snapdragon Compute, Snapdragon Consumer IOT, Snapdragon Consumer IOT, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon MobileSep-2110Possible buffer overflow due to improper validation of device types during P2P search in Snapdragon Auto, Snapdragon Consumer IOT, Snapdragon Mobile, Snapdragon Mobile, Snapdragon Mobile, Snapdragon Wired Infrastructure and Networking	Sep-21Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Industrial IOT, Snapdragon Wearablesqualcomm.co m/company/ product- security/bull etins/august- 2021-bulletinSep-212.1Snapdragon Consumer IOT, Snapdragon Mobile, Snapdragon WearablesCVE ID : CVE-2021-1929Sep-213.6Possible out of bounds read due to incorrect validation of incoming buffer length in Snapdragon Compute, Snapdragon Compute, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobilehttps://www. qualcomm.co m/company/ product- security/bull etins/august- 2021-bulletinSep-2110Possible buffer overflow due to improper validation of device types during P2P search in Snapdragon Auto, Snapdragon Consumer IOT, Snapdragon Nobilehttps://www. qualcomm.co m/company/ product- security/bull etins/august- 2021-bulletin

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2021-1972		
qcx315					
Exposure of Resource to Wrong Sphere	08-Sep-21	2.1	Child process can leak information from parent process due to numeric pids are getting compared and these pid can be reused in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables CVE ID : CVE-2021-1904	https://www. qualcomm.co m/company/ product- security/bull etins/august- 2021-bulletin	H-QUA-QCX3- 170921/1117
Loop with Unreachable Exit Condition ('Infinite Loop')	08-Sep-21	5	Loop with unreachable exit condition may occur due to improper handling of unsupported input in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Voice & Music, Snapdragon Wearables CVE ID : CVE-2021-1914	https://www. qualcomm.co m/company/ product- security/bull etins/august- 2021-bulletin	H-QUA-QCX3- 170921/1118
Out-of- bounds Write	08-Sep-21	10	Possible buffer underflow due to lack of check for negative indices values when processing user provided input in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT,	https://www. qualcomm.co m/company/ product- security/bull etins/august- 2021-bulletin	H-QUA-QCX3- 170921/1119

0-1

1-2

5-6

6-7

7-8

8-9

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Snapdragon IoT, Snapdragon Voice & Music, Snapdragon Wearables		
			CVE ID : CVE-2021-1916		
Integer Underflow (Wrap or Wraparoun d)	08-Sep-21	10	Integer underflow can occur when the RTCP length is lesser than than the actual blocks present in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Voice & Music, Snapdragon Wearables	https://www. qualcomm.co m/company/ product- security/bull etins/august- 2021-bulletin	H-QUA-QCX3- 170921/1120
			CVE ID : CVE-2021-1919		
Integer Underflow (Wrap or Wraparoun d)	08-Sep-21	10	Integer underflow can occur due to improper handling of incoming RTCP packets in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Voice & Music, Snapdragon Wearables	https://www. qualcomm.co m/company/ product- security/bull etins/august- 2021-bulletin	H-QUA-QCX3- 170921/1121
			CVE ID : CVE-2021-1920		
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	08-Sep-21	10	Possible buffer overflow due to improper validation of device types during P2P search in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music,	https://www. qualcomm.co m/company/ product- security/bull etins/august- 2021-bulletin	H-QUA-QCX3- 170921/1122

0-1

1-2

2-3 3-4

4-5

6-7

5-6

7-8

8-9

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking		
			CVE ID : CVE-2021-1972		
qet4101					I
Exposure of Resource to Wrong Sphere	08-Sep-21	2.1	Child process can leak information from parent process due to numeric pids are getting compared and these pid can be reused in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables CVE ID : CVE-2021-1904	https://www. qualcomm.co m/company/ product- security/bull etins/august- 2021-bulletin	H-QUA-QET4- 170921/1123
qfe1922					
Out-of- bounds Read	08-Sep-21	3.6	Buffer over read could occur due to incorrect check of buffer size while flashing emmc devices in Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking CVE ID : CVE-2021-1928	https://www. qualcomm.co m/company/ product- security/bull etins/august- 2021-bulletin	H-QUA-QFE1- 170921/1124
Buffer Copy without Checking Size of Input CVSS Scoring Sc	08-Sep-21 ale 0-1	10	Possible buffer overflow due to improper validation of device types during P2P search in Snapdragon Auto,	https://www. qualcomm.co m/company/ product-	H-QUA-QFE1- 170921/1125 8-9 9-10

Page 403 of 1474

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
('Classic Buffer Overflow')			Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking CVE ID : CVE-2021-1972	security/bull etins/august- 2021-bulletin	
qfe1952					
Out-of- bounds Read	08-Sep-21	3.6	Buffer over read could occur due to incorrect check of buffer size while flashing emmc devices in Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking CVE ID : CVE-2021-1928	https://www. qualcomm.co m/company/ product- security/bull etins/august- 2021-bulletin	H-QUA-QFE1- 170921/1126
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	08-Sep-21	10	Possible buffer overflow due to improper validation of device types during P2P search in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Woice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and	https://www. qualcomm.co m/company/ product- security/bull etins/august- 2021-bulletin	H-QUA-QFE1- 170921/1127

CVSS Scoring Scale	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10
			P	age 404 c	of 1474					

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Networking		
			CVE ID : CVE-2021-1972		
qrb5165					
Exposure of Resource to Wrong Sphere	08-Sep-21	2.1	Child process can leak information from parent process due to numeric pids are getting compared and these pid can be reused in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wearables CVE ID : CVE-2021-1904	https://www. qualcomm.co m/company/ product- security/bull etins/august- 2021-bulletin	H-QUA-QRB5- 170921/1128
Improper Restriction of Operations within the Bounds of a Memory Buffer	08-Sep-21	3.6	Possible out of bounds read due to incorrect validation of incoming buffer length in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile CVE ID : CVE-2021-1930	https://www. qualcomm.co m/company/ product- security/bull etins/august- 2021-bulletin	H-QUA-QRB5- 170921/1129
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	08-Sep-21	10	Possible buffer overflow due to improper validation of device types during P2P search in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables,	https://www. qualcomm.co m/company/ product- security/bull etins/august- 2021-bulletin	H-QUA-QRB5- 170921/1130
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 & CVE ID	Patch	NCIIPC ID
			Snapdragon Wired Infrastructure and Networking CVE ID : CVE-2021-1972		
qsm8250					
Exposure of Resource to Wrong Sphere	08-Sep-21	2.1	Child process can leak information from parent process due to numeric pids are getting compared and these pid can be reused in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wearables CVE ID : CVE-2021-1904	https://www. qualcomm.co m/company/ product- security/bull etins/august- 2021-bulletin	H-QUA-QSM8- 170921/1131
Improper Restriction of Operations within the Bounds of a Memory Buffer	08-Sep-21	3.6	Possible out of bounds read due to incorrect validation of incoming buffer length in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile CVE ID : CVE-2021-1930	https://www. qualcomm.co m/company/ product- security/bull etins/august- 2021-bulletin	H-QUA-QSM8- 170921/1132
qsm8350					
Incorrect Type Conversion or Cast	08-Sep-21	4.6	Incorrect pointer argument passed to trusted application TA could result in un- intended memory operations in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity,	https://www. qualcomm.co m/company/ product- security/bull etins/august- 2021-bulletin	H-QUA-QSM8- 170921/1133

CVSS	Scoring	Scale
C • 55	2001118	Jeane

Г

0-1

1-2

5-6

6-7

7-8

8-9

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Snapdragon Industrial IOT		
			CVE ID : CVE-2021-1923		
Improper Restriction of Operations within the Bounds of a Memory Buffer	08-Sep-21	3.6	Possible out of bounds read due to incorrect validation of incoming buffer length in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile CVE ID : CVE-2021-1930	https://www. qualcomm.co m/company/ product- security/bull etins/august- 2021-bulletin	H-QUA-QSM8- 170921/1134
qsw8573					
Exposure of Resource to Wrong Sphere	08-Sep-21	2.1	Child process can leak information from parent process due to numeric pids are getting compared and these pid can be reused in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables CVE ID : CVE-2021-1904	https://www. qualcomm.co m/company/ product- security/bull etins/august- 2021-bulletin	H-QUA- QSW8- 170921/1135
Loop with Unreachable Exit Condition ('Infinite Loop')	08-Sep-21	5	Loop with unreachable exit condition may occur due to improper handling of unsupported input in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Voice & Music, Snapdragon	https://www. qualcomm.co m/company/ product- security/bull etins/august- 2021-bulletin	H-QUA- QSW8- 170921/1136
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 & CVE ID	Patch	NCIIPC ID
			Wearables		
			CVE ID : CVE-2021-1914		
Out-of- bounds Write	08-Sep-21	10	Possible buffer underflow due to lack of check for negative indices values when processing user provided input in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Voice & Music, Snapdragon Wearables	https://www. qualcomm.co m/company/ product- security/bull etins/august- 2021-bulletin	H-QUA- QSW8- 170921/1137
			CVE ID : CVE-2021-1916		
Integer Underflow (Wrap or Wraparoun d)	08-Sep-21	10	Integer underflow can occur when the RTCP length is lesser than than the actual blocks present in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Voice & Music, Snapdragon Wearables CVE ID : CVE-2021-1919	https://www. qualcomm.co m/company/ product- security/bull etins/august- 2021-bulletin	H-QUA- QSW8- 170921/1138
Integer Underflow (Wrap or Wraparoun d)	08-Sep-21	10	Integer underflow can occur due to improper handling of incoming RTCP packets in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Voice & Music, Snapdragon Wearables	https://www. qualcomm.co m/company/ product- security/bull etins/august- 2021-bulletin	H-QUA- QSW8- 170921/1139
CVSS Scoring Sca	ale 0-1	1-2	2-3 3-4 4-5 5-6	6-7 7-8	8-9 9-10

Page 408 of 1474

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2021-1920		
qualcomm21	15			I	
Exposure of Resource to Wrong Sphere	08-Sep-21	2.1	Child process can leak information from parent process due to numeric pids are getting compared and these pid can be reused in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables CVE ID : CVE-2021-1904	https://www. qualcomm.co m/company/ product- security/bull etins/august- 2021-bulletin	H-QUA-QUAL- 170921/1140
Loop with Unreachable Exit Condition ('Infinite Loop')	08-Sep-21	5	Loop with unreachable exit condition may occur due to improper handling of unsupported input in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Voice & Music, Snapdragon Wearables CVE ID : CVE-2021-1914	https://www. qualcomm.co m/company/ product- security/bull etins/august- 2021-bulletin	H-QUA-QUAL- 170921/1141
Out-of- bounds Write	08-Sep-21	10	Possible buffer underflow due to lack of check for negative indices values when processing user provided input in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT,	https://www. qualcomm.co m/company/ product- security/bull etins/august- 2021-bulletin	H-QUA-QUAL- 170921/1142

0-1

1-2

5-6

6-7

7-8

8-9

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Snapdragon IoT, Snapdragon Voice & Music, Snapdragon Wearables		
			CVE ID : CVE-2021-1916		
Integer Underflow (Wrap or Wraparoun d)	08-Sep-21	10	Integer underflow can occur when the RTCP length is lesser than than the actual blocks present in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Voice & Music, Snapdragon Wearables CVE ID : CVE-2021-1919	https://www. qualcomm.co m/company/ product- security/bull etins/august- 2021-bulletin	H-QUA-QUAL- 170921/1143
Integer Underflow (Wrap or Wraparoun d)	08-Sep-21	10	Integer underflow can occur due to improper handling of incoming RTCP packets in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Voice & Music, Snapdragon Wearables	https://www. qualcomm.co m/company/ product- security/bull etins/august- 2021-bulletin	H-QUA-QUAL- 170921/1144
			CVE ID : CVE-2021-1920		
Out-of- bounds Read	08-Sep-21	3.6	Buffer over read could occur due to incorrect check of buffer size while flashing emmc devices in Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon	https://www. qualcomm.co m/company/ product- security/bull etins/august- 2021-bulletin	H-QUA-QUAL- 170921/1145

1	CVSS Scoring Scale	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10
	CV35 Scotting Scale	01	12	23	5 4	ΨJ	50	07	70	05	5 10
				D	aga 110 c	f 1 / 7 /					

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Wired Infrastructure and Networking CVE ID : CVE-2021-1928		
Exposure of Resource to Wrong Sphere	08-Sep-21	2.1	Lack of strict validation of bootmode can lead to information disclosure in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wearables CVE ID : CVE-2021-1929	https://www. qualcomm.co m/company/ product- security/bull etins/august- 2021-bulletin	H-QUA-QUAL- 170921/1146
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	08-Sep-21	10	Possible buffer overflow due to improper validation of device types during P2P search in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Woice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking CVE ID : CVE-2021-1972	https://www. qualcomm.co m/company/ product- security/bull etins/august- 2021-bulletin	H-QUA-QUAL- 170921/1147
sa415m				<u> </u>	
Exposure of Resource to Wrong Sphere	08-Sep-21	2.1	Child process can leak information from parent process due to numeric pids are getting compared and these pid can be reused in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity,	https://www. qualcomm.co m/company/ product- security/bull etins/august- 2021-bulletin	H-QUA-SA41- 170921/1148
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 & CVE ID	Patch	NCIIPC ID
			Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables CVE ID : CVE-2021-1904		
Loop with Unreachable Exit Condition ('Infinite Loop')	08-Sep-21	5	Loop with unreachable exit condition may occur due to improper handling of unsupported input in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Voice & Music, Snapdragon Wearables CVE ID : CVE-2021-1914	https://www. qualcomm.co m/company/ product- security/bull etins/august- 2021-bulletin	H-QUA-SA41- 170921/1149
Out-of- bounds Write	08-Sep-21	10	Possible buffer underflow due to lack of check for negative indices values when processing user provided input in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Voice & Music, Snapdragon Wearables CVE ID : CVE-2021-1916	https://www. qualcomm.co m/company/ product- security/bull etins/august- 2021-bulletin	H-QUA-SA41- 170921/1150
Integer Underflow (Wrap or Wraparoun d)	08-Sep-21	10	Integer underflow can occur when the RTCP length is lesser than than the actual blocks present in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity,	https://www. qualcomm.co m/company/ product- security/bull etins/august-	H-QUA-SA41- 170921/1151

1-2

0-1

6-7

5-6

7-8

8-9

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Voice & Music, Snapdragon Wearables CVE ID : CVE-2021-1919	2021-bulletin	
Integer Underflow (Wrap or Wraparoun d)	08-Sep-21	10	Integer underflow can occur due to improper handling of incoming RTCP packets in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Voice & Music, Snapdragon Wearables CVE ID : CVE-2021-1920	https://www. qualcomm.co m/company/ product- security/bull etins/august- 2021-bulletin	H-QUA-SA41- 170921/1152
Improper Restriction of Operations within the Bounds of a Memory Buffer	08-Sep-21	3.6	Possible out of bounds read due to incorrect validation of incoming buffer length in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile CVE ID : CVE-2021-1930	https://www. qualcomm.co m/company/ product- security/bull etins/august- 2021-bulletin	H-QUA-SA41- 170921/1153
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	08-Sep-21	10	Possible buffer overflow due to improper validation of device types during P2P search in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music,	https://www. qualcomm.co m/company/ product- security/bull etins/august- 2021-bulletin	H-QUA-SA41- 170921/1154

1-2

0-1

6-7

5-6

7-8

8-9

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking		
			CVE ID : CVE-2021-1972		
sa515m					
Loop with Unreachable Exit Condition ('Infinite Loop')	08-Sep-21	5	Loop with unreachable exit condition may occur due to improper handling of unsupported input in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Voice & Music, Snapdragon Wearables CVE ID : CVE-2021-1914	https://www. qualcomm.co m/company/ product- security/bull etins/august- 2021-bulletin	H-QUA-SA51- 170921/1155
Out-of- bounds Write	08-Sep-21	10	Possible buffer underflow due to lack of check for negative indices values when processing user provided input in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Voice & Music, Snapdragon Wearables CVE ID : CVE-2021-1916	https://www. qualcomm.co m/company/ product- security/bull etins/august- 2021-bulletin	H-QUA-SA51- 170921/1156
Integer Underflow (Wrap or Wraparoun d)	08-Sep-21	10	Integer underflow can occur when the RTCP length is lesser than than the actual blocks present in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity,	https://www. qualcomm.co m/company/ product- security/bull etins/august-	H-QUA-SA51- 170921/1157
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 & CVE ID	Patch	NCIIPC ID
			Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Voice & Music, Snapdragon Wearables CVE ID : CVE-2021-1919	2021-bulletin	
Integer Underflow (Wrap or Wraparoun d)	08-Sep-21	10	Integer underflow can occur due to improper handling of incoming RTCP packets in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Voice & Music, Snapdragon Wearables	https://www. qualcomm.co m/company/ product- security/bull etins/august- 2021-bulletin	H-QUA-SA51- 170921/1158
			CVE ID : CVE-2021-1920		
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	08-Sep-21	10	Possible buffer overflow due to improper validation of device types during P2P search in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Woice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking CVE ID : CVE-2021-1972	https://www. qualcomm.co m/company/ product- security/bull etins/august- 2021-bulletin	H-QUA-SA51- 170921/1159
sa6145p					
Exposure of Resource to Wrong Sphere	08-Sep-21	2.1	Child process can leak information from parent process due to numeric pids are getting compared and	https://www. qualcomm.co m/company/ product-	H-QUA-SA61- 170921/1160
CVSS Scoring Sc	ale 0-1	1-2	2-3 3-4 4-5 5-6 Page 415 of 1474	6-7 7-8	8-9 9-10

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			these pid can be reused in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables CVE ID : CVE-2021-1904	security/bull etins/august- 2021-bulletin	
Out-of- bounds Write	08-Sep-21	10	Possible buffer underflow due to lack of check for negative indices values when processing user provided input in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Voice & Music, Snapdragon Wearables CVE ID : CVE-2021-1916	https://www. qualcomm.co m/company/ product- security/bull etins/august- 2021-bulletin	H-QUA-SA61- 170921/1161
Incorrect Type Conversion or Cast	08-Sep-21	4.6	Incorrect pointer argument passed to trusted application TA could result in un- intended memory operations in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Industrial IOT CVE ID : CVE-2021-1923	https://www. qualcomm.co m/company/ product- security/bull etins/august- 2021-bulletin	H-QUA-SA61- 170921/1162
Exposure of Resource to Wrong Sphere	08-Sep-21	2.1	Lack of strict validation of bootmode can lead to information disclosure in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity,	https://www. qualcomm.co m/company/ product- security/bull etins/august-	H-QUA-SA61- 170921/1163

1-2 2-3

0-1

6-7

5-6

7-8

8-9

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wearables	2021-bulletin	
			CVE ID : CVE-2021-1929		
Improper Restriction of Operations within the Bounds of a Memory Buffer	08-Sep-21	3.6	Possible out of bounds read due to incorrect validation of incoming buffer length in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile	https://www. qualcomm.co m/company/ product- security/bull etins/august- 2021-bulletin	H-QUA-SA61- 170921/1164
			CVE ID : CVE-2021-1930		
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	08-Sep-21	10	Possible buffer overflow due to improper validation of device types during P2P search in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Woice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking CVE ID : CVE-2021-1972	https://www. qualcomm.co m/company/ product- security/bull etins/august- 2021-bulletin	H-QUA-SA61- 170921/1165
sa6150p					
Exposure of Resource to Wrong Sphere	08-Sep-21	2.1	Child process can leak information from parent process due to numeric pids are getting compared and these pid can be reused in Snapdragon Auto, Snapdragon Compute,	https://www. qualcomm.co m/company/ product- security/bull etins/august- 2021-bulletin	H-QUA-SA61- 170921/1166
CVSS Scoring Sc	ale 0-1	1-2	2-3 3-4 4-5 5-6 Page 417 of 1474	6-7 7-8	8-9 9-10

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables CVE ID : CVE-2021-1904		
Out-of- bounds Write	08-Sep-21	10	Possible buffer underflow due to lack of check for negative indices values when processing user provided input in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Voice & Music, Snapdragon Wearables CVE ID : CVE-2021-1916	https://www. qualcomm.co m/company/ product- security/bull etins/august- 2021-bulletin	H-QUA-SA61- 170921/1167
Incorrect Type Conversion or Cast	08-Sep-21	4.6	Incorrect pointer argument passed to trusted application TA could result in un- intended memory operations in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Industrial IOT CVE ID : CVE-2021-1923	https://www. qualcomm.co m/company/ product- security/bull etins/august- 2021-bulletin	H-QUA-SA61- 170921/1168
Exposure of Resource to Wrong Sphere	08-Sep-21	2.1	Lack of strict validation of bootmode can lead to information disclosure in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile,	https://www. qualcomm.co m/company/ product- security/bull etins/august- 2021-bulletin	H-QUA-SA61- 170921/1169

1-2 2-3

0-1

4-5

6-7

5-6

7-8

8-9

9-10

Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
		Snapdragon Wearables		
		CVE ID : CVE-2021-1929		
08-Sep-21	3.6	Possible out of bounds read due to incorrect validation of incoming buffer length in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile CVE ID : CVE-2021-1930	https://www. qualcomm.co m/company/ product- security/bull etins/august- 2021-bulletin	H-QUA-SA61- 170921/1170
08-Sep-21	10	Possible buffer overflow due to improper validation of device types during P2P search in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Woice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking CVE ID : CVE-2021-1972	https://www. qualcomm.co m/company/ product- security/bull etins/august- 2021-bulletin	H-QUA-SA61- 170921/1171
08-Sep-21	2.1	Child process can leak information from parent process due to numeric pids are getting compared and these pid can be reused in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT,	https://www. qualcomm.co m/company/ product- security/bull etins/august- 2021-bulletin	H-QUA-SA61- 170921/1172
	08-Sep-21	Image: marked biase of the second state of the second s	Image: construct of the second seco	Image: constraint of the second sec

Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
		Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables		
08-Sep-21	10	due to lack of check for negative indices values when processing user provided input in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Voice & Music, Snapdragon Wearables	https://www. qualcomm.co m/company/ product- security/bull etins/august- 2021-bulletin	H-QUA-SA61- 170921/1173
08-Sep-21	4.6	Incorrect pointer argument passed to trusted application TA could result in un- intended memory operations in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Industrial IOT CVE ID : CVE-2021-1923	https://www. qualcomm.co m/company/ product- security/bull etins/august- 2021-bulletin	H-QUA-SA61- 170921/1174
08-Sep-21	3.6	Possible out of bounds read due to incorrect validation of incoming buffer length in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile CVE ID : CVE-2021-1930	https://www. qualcomm.co m/company/ product- security/bull etins/august- 2021-bulletin	H-QUA-SA61- 170921/1175
08-Sep-21	10	Possible buffer overflow due to improper validation of	https://www. qualcomm.co	H-QUA-SA61-
	08-Sep-21 08-Sep-21	08-Sep-21 10 08-Sep-21 4.6 08-Sep-21 3.6	08-Sep-210008-Sep-214.6Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables08-Sep-217Possible buffer underflow due to lack of check for negative indices values when processing user provided input in Snapdragon Auto, Snapdragon Conpute, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Compute, Snapdragon Industrial IOT, Snapdragon Auto, Snapdragon Industrial IOT, Snapdragon Industrial IOT, Snap	08-Sep-21A.6Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon WearablesHttps://www. qualcomm.co m/company/ product- security/bull etins/august- 2021-bulletin08-Sep-2110Incorrect pointer argument passed to trusted application instradragon Auto, Snapdragon Industrial IOT, Snapdragon Industrial IOT Product- security/bull etins/august- 2021-bulletin08-Sep-214.608-Sep-213.608-Sep-219.008-Sep-213.608-Sep-211008-Sep-211008-Sep-211008-Sep-211008-Sep-211008-Sep-211008-Sep-211008-Sep-211008-Sep-211008-Sep-211008-Sep-211008-Sep-211008-Sep-211008-Sep-211008-Sep-211008-Sep-211008-Sep-211008-Sep-211008-Sep-21<

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Checking Size of Input ('Classic Buffer Overflow')			device types during P2P search in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Woice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking CVE ID : CVE-2021-1972	m/company/ product- security/bull etins/august- 2021-bulletin	170921/1176
sa6155p					
Exposure of Resource to Wrong Sphere	08-Sep-21	2.1	Child process can leak information from parent process due to numeric pids are getting compared and these pid can be reused in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wearables CVE ID : CVE-2021-1904	https://www. qualcomm.co m/company/ product- security/bull etins/august- 2021-bulletin	H-QUA-SA61- 170921/1177
Out-of- bounds Write	08-Sep-21	10	Possible buffer underflow due to lack of check for negative indices values when processing user provided input in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Voice & Music, Snapdragon	https://www. qualcomm.co m/company/ product- security/bull etins/august- 2021-bulletin	H-QUA-SA61- 170921/1178

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Wearables		
			CVE ID : CVE-2021-1916		
Incorrect Type Conversion or Cast	08-Sep-21	4.6	Incorrect pointer argument passed to trusted application TA could result in un- intended memory operations in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Industrial IOT CVE ID : CVE-2021-1923	https://www. qualcomm.co m/company/ product- security/bull etins/august- 2021-bulletin	H-QUA-SA61- 170921/1179
Exposure of Resource to Wrong Sphere	08-Sep-21	2.1	Lack of strict validation of bootmode can lead to information disclosure in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wearables CVE ID : CVE-2021-1929	https://www. qualcomm.co m/company/ product- security/bull etins/august- 2021-bulletin	H-QUA-SA61- 170921/1180
Improper Restriction of Operations within the Bounds of a Memory Buffer	08-Sep-21	3.6	Possible out of bounds read due to incorrect validation of incoming buffer length in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile CVE ID : CVE-2021-1930	https://www. qualcomm.co m/company/ product- security/bull etins/august- 2021-bulletin	H-QUA-SA61- 170921/1181
Buffer Copy without Checking Size of Input ('Classic Buffer CVSS Scoring Sc	08-Sep-21	10	Possible buffer overflow due to improper validation of device types during P2P search in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity,	https://www. qualcomm.co m/company/ product- security/bull etins/august-	H-QUA-SA61- 170921/1182 8-9 9-10

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Overflow')			Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking CVE ID : CVE-2021-1972	2021-bulletin	
sa8145p					
Exposure of Resource to Wrong Sphere	08-Sep-21	2.1	Child process can leak information from parent process due to numeric pids are getting compared and these pid can be reused in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables CVE ID : CVE-2021-1904	https://www. qualcomm.co m/company/ product- security/bull etins/august- 2021-bulletin	H-QUA-SA81- 170921/1183
Out-of- bounds Write	08-Sep-21	10	Possible buffer underflow due to lack of check for negative indices values when processing user provided input in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Voice & Music, Snapdragon Wearables CVE ID : CVE-2021-1916	https://www. qualcomm.co m/company/ product- security/bull etins/august- 2021-bulletin	H-QUA-SA81- 170921/1184
Incorrect	08-Sep-21	4.6	Incorrect pointer argument	https://www.	H-QUA-SA81-
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 & CVE ID	Patch	NCIIPC ID
Type Conversion or Cast			passed to trusted application TA could result in un- intended memory operations in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Industrial IOT CVE ID : CVE-2021-1923	qualcomm.co m/company/ product- security/bull etins/august- 2021-bulletin	170921/1185
Exposure of Resource to Wrong Sphere	08-Sep-21	2.1	Lack of strict validation of bootmode can lead to information disclosure in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wearables CVE ID : CVE-2021-1929	https://www. qualcomm.co m/company/ product- security/bull etins/august- 2021-bulletin	H-QUA-SA81- 170921/1186
Improper Restriction of Operations within the Bounds of a Memory Buffer	08-Sep-21	3.6	Possible out of bounds read due to incorrect validation of incoming buffer length in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile CVE ID : CVE-2021-1930	https://www. qualcomm.co m/company/ product- security/bull etins/august- 2021-bulletin	H-QUA-SA81- 170921/1187
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	08-Sep-21	10	Possible buffer overflow due to improper validation of device types during P2P search in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile,	https://www. qualcomm.co m/company/ product- security/bull etins/august- 2021-bulletin	H-QUA-SA81- 170921/1188

0-1 1-2

5-6

6-7

7-8

8-9

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking CVE ID : CVE-2021-1972		
sa8150p					
Exposure of Resource to Wrong Sphere	08-Sep-21	2.1	Child process can leak information from parent process due to numeric pids are getting compared and these pid can be reused in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wearables CVE ID : CVE-2021-1904	https://www. qualcomm.co m/company/ product- security/bull etins/august- 2021-bulletin	H-QUA-SA81- 170921/1189
Out-of- bounds Write	08-Sep-21	10	Possible buffer underflow due to lack of check for negative indices values when processing user provided input in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Voice & Music, Snapdragon Wearables CVE ID : CVE-2021-1916	https://www. qualcomm.co m/company/ product- security/bull etins/august- 2021-bulletin	H-QUA-SA81- 170921/1190
Incorrect Type Conversion or Cast	08-Sep-21	4.6	Incorrect pointer argument passed to trusted application TA could result in un- intended memory operations	https://www. qualcomm.co m/company/ product-	H-QUA-SA81- 170921/1191
CVSS Scoring Sco	ale 0-1	1-2	2-3 3-4 4-5 5-6	6-7 7-8	8-9 <mark>9-10</mark>

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Industrial IOT CVE ID : CVE-2021-1923	security/bull etins/august- 2021-bulletin	
Exposure of Resource to Wrong Sphere	08-Sep-21	2.1	Lack of strict validation of bootmode can lead to information disclosure in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wearables CVE ID : CVE-2021-1929	https://www. qualcomm.co m/company/ product- security/bull etins/august- 2021-bulletin	H-QUA-SA81- 170921/1192
Improper Restriction of Operations within the Bounds of a Memory Buffer	08-Sep-21	3.6	Possible out of bounds read due to incorrect validation of incoming buffer length in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile CVE ID : CVE-2021-1930	https://www. qualcomm.co m/company/ product- security/bull etins/august- 2021-bulletin	H-QUA-SA81- 170921/1193
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	08-Sep-21	10	Possible buffer overflow due to improper validation of device types during P2P search in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Woice & Music, Snapdragon Wearables, Snapdragon Wired	https://www. qualcomm.co m/company/ product- security/bull etins/august- 2021-bulletin	H-QUA-SA81- 170921/1194

0-1

1-2

6-7

5-6

7-8

8-9

Image: Infrastructure and Networking CVE ID : CVE-2021-1972Image: Image: I	Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
CVE ID : CVE-2021-1972sa8155Exposure of Resource to Wrong Sphere08-Sep-21Child process can leak information from parent process due to numeric pids are getting compared and these pid can be reused in Snapdragon Compute, Snapdragon Consumer 10T, Snapdragon Consumer 10T, Snapdragon Industrial 10T, Snapdragon Nobile, Snapdragon Nobile, Snapdragon Nobile, Snapdragon Mearableshttps://www. qualcomm.co m/company/ product- security/bull etins/august- 2021-bulletinH-QUA-SA81- 170921/1195Loop with Unreachable Exit Condition ('Infinite Loop')08-Sep-215Sapdragon Compute, Snapdragon Mearables CVE ID : CVE-2021-1904https://www. qualcomm.co m/company/ product- security/bull etins/august- 2021-bulletinH-QUA-SA81- 170921/11950ut-of- bounds08-Sep-215Sapdragon Compute, Snapdragon Consumer 10T, Snapdragon Consumer 10T, Snapdragon Consumer 10T, Snapdragon Consumer 10T, Snapdragon Consumer 10T, Snapdragon Industrial 10T, Snapdragon Consumer 10T, Snapdragon Consumer 10T, Snapdragon Industrial 10T, Snapdragon Consumer 10T, Snapdragon Industrial 10T, Snapdragon Consumer 10T, Snapdragon Industrial 10T, Snapdragon Nee Sonapdragon N						
sa8155Exposure of Resource to Wrong Sphere08-Sep-212.1Child process can leak information from parent process due to numeric pids are getting compared and these pid can be reused in Snapdragon Connectivity, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Voice & Music, Snapdragon Connectivity, Snapdragon Nobile, Snapdragon Voice & Music, Snapdragon Nobile, Snapdragon Consumer IOT, Snapdragon Consumer IOT, Snapdragon Consumer IOT, Snapdragon Consumer IOT, Snapdragon Consumer IOT, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon IoT, Snapdragon IoT, Snapdragon IoT, Snapdragon IoT, Snapdragon Voice & Music, Snapdragon IoT, Snapdragon Snapdragon IoT, Snapdragon Voice & Music, Snapdragon Snapdragon IoT, Snapdragon Voice & Music, Snapdragon Snapdragon IoT, Snapdragon Voice & Music, Snapdragon Muto, Snapdragon Compute, Nittps://www. H-QUA-SA81-170921/1197H-QUA-SA81-170921/1196Out-of- bounds Write08-Sep-2110Possible buffer underflow due to lack of check f				0		
Exposure of Resource to Wrong Sphere08-Sep-2114Child process can leak information from parent process due to numeric pids are getting compared and these pid can be reused in Snapdragon Consumer IOT, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Nobile, Snapdragon Voice & Music, Snapdragon Wearableshttps://www. qualcomm.co m/company/ product- security/bull 2021-bulletinH-QUA-SA81- 170921/1195Loop with Unreachable Exit Condition (Infinite Loop')08-Sep-215Loop with unreachable exit condition may occur due to improper handling of unsuppred input in Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IOT, Snapdragon Voice & Music, Snapdragon Auto, scurity/bull etarity/bull etarity/bull etarity/bull etarity/bull etarity/bull etarity/bull etarity/bull etarity/bull etarity/bull etarity/bull etarity/bullH-QUA-SA81- 170921/1190Out-of-<	0155			CVE ID : CVE-2021-1972		
Exposure of Resource to Wrong Sphere08-Sep-212.1information from parent process due to numeric pids are getting compared and these pid can be reused in Snapdragon Connectivity, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Mobile, Snapdragon Nobile, Snapdragon Voice & Music, Snapdragon Voice & Music, Snapdragon Nobile, Snapdragon Nobile, Snapdragon Nobile, Snapdragon Connectivity, Snapdragon Nobile, Snapdragon Nobile, Snapdragon Connectivity, Snapdragon Nobile, Snapdragon Nobile, Snapdragon Connectivity, Snapdragon Nobile, Snapdragon Nobile, Snapdragon Nobile, Snapdragon Connectivity, Snapdragon Connectivity, Snapdragon Connectivity, Snapdragon Nobile, Snapdragon Connectivity, Snapdragon Nobile, Snapdragon Connectivity, Snapdragon Connectivity, Snapdragon Connectivity, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Consumer IOT, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Consumer IOT, Snapdragon Consumer IOT, Snapdragon Consumer IOT, Snapdragon Consumer IOT, Snapdragon Consumer IOT, Snapdragon Industrial IOT, <td>sa8155</td> <td></td> <td></td> <td></td> <td></td> <td></td>	sa8155					
Loop with Unreachable Exit Condition 	Resource to Wrong	08-Sep-21	2.1	information from parent process due to numeric pids are getting compared and these pid can be reused in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wearables	qualcomm.co m/company/ product- security/bull etins/august-	=
Out-of- bounds Write08-Sep-2110Image: Construct of the charge o	Unreachable Exit Condition ('Infinite	08-Sep-21	5	condition may occur due to improper handling of unsupported input in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Voice & Music, Snapdragon Wearables	qualcomm.co m/company/ product- security/bull etins/august-	-
Snapdragon Connectivity, 2021-bulletin	bounds	08-Sep-21	10	due to lack of check for negative indices values when processing user provided input in Snapdragon Auto,	qualcomm.co m/company/ product- security/bull	-

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Voice & Music, Snapdragon Wearables		
			CVE ID : CVE-2021-1916		
Integer Underflow (Wrap or Wraparoun d)	08-Sep-21	10	Integer underflow can occur when the RTCP length is lesser than than the actual blocks present in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Voice & Music, Snapdragon Wearables	https://www. qualcomm.co m/company/ product- security/bull etins/august- 2021-bulletin	H-QUA-SA81- 170921/1198
			CVE ID : CVE-2021-1919		
Integer Underflow (Wrap or Wraparoun d)	08-Sep-21	10	Integer underflow can occur due to improper handling of incoming RTCP packets in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Voice & Music, Snapdragon Wearables	https://www. qualcomm.co m/company/ product- security/bull etins/august- 2021-bulletin	H-QUA-SA81- 170921/1199
			CVE ID : CVE-2021-1920		
Incorrect Type Conversion or Cast	08-Sep-21	4.6	Incorrect pointer argument passed to trusted application TA could result in un- intended memory operations in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Industrial IOT	https://www. qualcomm.co m/company/ product- security/bull etins/august- 2021-bulletin	H-QUA-SA81- 170921/1200
CVSS Scoring Sco	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-2021-1923		
Exposure of Resource to Wrong Sphere	08-Sep-21	2.1	Lack of strict validation of bootmode can lead to information disclosure in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wearables CVE ID : CVE-2021-1929	https://www. qualcomm.co m/company/ product- security/bull etins/august- 2021-bulletin	H-QUA-SA81- 170921/1201
Improper Restriction of Operations within the Bounds of a Memory Buffer	08-Sep-21	3.6	Possible out of bounds read due to incorrect validation of incoming buffer length in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile CVE ID : CVE-2021-1930	https://www. qualcomm.co m/company/ product- security/bull etins/august- 2021-bulletin	H-QUA-SA81- 170921/1202
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	08-Sep-21	10	Possible buffer overflow due to improper validation of device types during P2P search in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Industrial IOT, Snapdragon Woile, Snapdragon Woile, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking CVE ID : CVE-2021-1972	https://www. qualcomm.co m/company/ product- security/bull etins/august- 2021-bulletin	H-QUA-SA81- 170921/1203
sa8155p					
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 & CVE ID	Patch	NCIIPC ID
Exposure of Resource to Wrong Sphere	08-Sep-21	2.1	Child process can leak information from parent process due to numeric pids are getting compared and these pid can be reused in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wearables CVE ID : CVE-2021-1904	https://www. qualcomm.co m/company/ product- security/bull etins/august- 2021-bulletin	H-QUA-SA81- 170921/1204
Loop with Unreachable Exit Condition ('Infinite Loop')	08-Sep-21	5	Loop with unreachable exit condition may occur due to improper handling of unsupported input in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Voice & Music, Snapdragon Wearables CVE ID : CVE-2021-1914	https://www. qualcomm.co m/company/ product- security/bull etins/august- 2021-bulletin	H-QUA-SA81- 170921/1205
Out-of- bounds Write	08-Sep-21	10	Possible buffer underflow due to lack of check for negative indices values when processing user provided input in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Voice & Music, Snapdragon Wearables	https://www. qualcomm.co m/company/ product- security/bull etins/august- 2021-bulletin	H-QUA-SA81- 170921/1206
CVSS Scoring Sc	ale 0-1	2-3 3-4 4-5 5-6 Page 430 of 1474	6-7 7-8	8-9 9-10	

Page 430 of 1474

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2021-1916		
Integer Underflow (Wrap or Wraparoun d)	08-Sep-21	10	Integer underflow can occur when the RTCP length is lesser than than the actual blocks present in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Voice & Music, Snapdragon Wearables CVE ID : CVE-2021-1919	https://www. qualcomm.co m/company/ product- security/bull etins/august- 2021-bulletin	H-QUA-SA81- 170921/1207
Integer Underflow (Wrap or Wraparoun d)	08-Sep-21	10	Integer underflow can occur due to improper handling of incoming RTCP packets in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Voice & Music, Snapdragon Wearables CVE ID : CVE-2021-1920	https://www. qualcomm.co m/company/ product- security/bull etins/august- 2021-bulletin	H-QUA-SA81- 170921/1208
Incorrect Type Conversion or Cast	08-Sep-21	4.6	Incorrect pointer argument passed to trusted application TA could result in un- intended memory operations in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Industrial IOT CVE ID : CVE-2021-1923	https://www. qualcomm.co m/company/ product- security/bull etins/august- 2021-bulletin	H-QUA-SA81- 170921/1209
Exposure of Resource to Wrong Sphere CVSS Scoring Sc	08-Sep-21 ale 0-1	2.1	Lack of strict validation of bootmode can lead to information disclosure in Snapdragon Auto, 2-3 3-4 4-5 5-6	https://www. qualcomm.co m/company/ product-	H-QUA-SA81- 170921/1210 8-9 9-10

Page 431 of 1474

98-Sep-21	3.6	Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wearables CVE ID : CVE-2021-1929 Possible out of bounds read due to incorrect validation of incoming buffer length in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Industrial IOT, Snapdragon Mobile	security/bull etins/august- 2021-bulletin https://www. qualcomm.co m/company/ product- security/bull etins/august-	H-QUA-SA81- 170921/1211
)8-Sep-21	3.6	Possible out of bounds read due to incorrect validation of incoming buffer length in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT,	qualcomm.co m/company/ product- security/bull etins/august-	-
)8-Sep-21	3.6	due to incorrect validation of incoming buffer length in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT,	qualcomm.co m/company/ product- security/bull etins/august-	-
		CVE ID : CVE-2021-1930	2021-bulletin	
)8-Sep-21	10	Possible buffer overflow due to improper validation of device types during P2P search in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Woice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking CVE ID : CVE-2021-1972	https://www. qualcomm.co m/company/ product- security/bull etins/august- 2021-bulletin	H-QUA-SA81- 170921/1212
98-Sep-21	2.1	Child process can leak information from parent process due to numeric pids are getting compared and these pid can be reused in	https://www. qualcomm.co m/company/ product- security/bull	H-QUA-SA81- 170921/1213
		3-Sep-21 2.1	3-Sep-2110device types during P2P search in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking CVE ID : CVE-2021-19723-Sep-212.1Child process can leak information from parent process due to numeric pids are getting compared and these pid can be reused in	3-Sep-2110device types during P2P search in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking CVE ID : CVE-2021-1972https://www. qualcomm.co m/company/ product- security/bull etins/august- 2021-bulletin3-Sep-212.1Child process can leak information from parent process due to numeric pids are getting compared and these pid can be reused inhttps://www. qualcomm.co m/company/ product- security/bull

				NCIIPC ID
		Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables CVE ID : CVE-2021-1904	etins/august- 2021-bulletin	
08-Sep-21	10	Possible buffer underflow due to lack of check for negative indices values when processing user provided input in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Voice & Music, Snapdragon Wearables CVE ID : CVE-2021-1916	https://www. qualcomm.co m/company/ product- security/bull etins/august- 2021-bulletin	H-QUA-SA81- 170921/1214
08-Sep-21	4.6	Incorrect pointer argument passed to trusted application TA could result in un- intended memory operations in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Industrial IOT CVE ID : CVE-2021-1923	https://www. qualcomm.co m/company/ product- security/bull etins/august- 2021-bulletin	H-QUA-SA81- 170921/1215
08-Sep-21	2.1	Lack of strict validation of bootmode can lead to information disclosure in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT,	https://www. qualcomm.co m/company/ product- security/bull etins/august- 2021-bulletin	H-QUA-SA81- 170921/1216
	08-Sep-21	08-Sep-21 4.6 08-Sep-21 2.1	08-Sep-21Interference 4.6Snapdragon Connectivity, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables08-Sep-21Interference 4.6Possible buffer underflow due to lack of check for negative indices values when processing user provided input in Snapdragon Auto, Snapdragon Compute, Snapdragon Industrial IOT, Snapdragon Compute, Snapdragon Industrial IOT, Snapdragon Compute, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Auto, Snapdragon Compute, Snapdragon Industrial IOT ITA could result in un- intended memory operations in Snapdragon Industrial IOT Ita could result in Un- intended memory operations in Snapdragon Industrial IOT Ita could result in Un- intended memory operations in Snapdragon Industrial IOT Ita could result in Un- intended memory operations in Snapdragon Industrial IOT Ita could result in Un- intended memory operations in Snapdragon Industrial IOT Ita could result in Un- intended memory operations in Snapdragon Industrial IOT Ita could result in Un- intended memory operations in Snapdragon Industrial IOT Ita could result in Un- intended memory operations in Snapdragon Industrial IOT Ita could result in Un- intended mem	08-Sep-21Sapadragon Connectivity, Snapdragon Nobile, Snapdragon Voice & Music, Snapdragon Voice & Music, Snapdragon Voice & Music, Snapdragon Vearableshttps://www. qualcomm.co m/company/ product- security/bull etins/august- 2021-bulletin08-Sep-2110Incorrect pointer argument passed to trusted application in Snapdragon Connectivity, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Consumer IOT, Snapdragon Consumer IOT, Snapdragon Consumer IOT, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Industrial IOT, Snapdragon Industrial IOT, Snapdragon Consumer IOT, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Consumer IOT, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Industrial IOT, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Consumer IOT, Snapdragon Consumer IOT, Snapdragon Connectivity, Snapdragon Connectivity, Snapdragon Connectivity, Snapdragon Connectivity, Snapdragon Connectivity, Snapdragon Connectivity, Snapdragon Industrial IOT, Snapdragon Connectivity, Snapdragon Connectiv

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wearables		
			CVE ID : CVE-2021-1929		
Improper Restriction of Operations within the Bounds of a Memory Buffer	08-Sep-21	3.6	Possible out of bounds read due to incorrect validation of incoming buffer length in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile	https://www. qualcomm.co m/company/ product- security/bull etins/august- 2021-bulletin	H-QUA-SA81- 170921/1217
			CVE ID : CVE-2021-1930		
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	08-Sep-21	10	Possible buffer overflow due to improper validation of device types during P2P search in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Woice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking CVE ID : CVE-2021-1972	https://www. qualcomm.co m/company/ product- security/bull etins/august- 2021-bulletin	H-QUA-SA81- 170921/1218
sc8180x					
Loop with Unreachable Exit Condition ('Infinite Loop')	08-Sep-21	5	Loop with unreachable exit condition may occur due to improper handling of unsupported input in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT,	https://www. qualcomm.co m/company/ product- security/bull etins/august- 2021-bulletin	H-QUA-SC81- 170921/1219
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 & CVE ID	Patch	NCIIPC ID
			Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Voice & Music, Snapdragon Wearables CVE ID : CVE-2021-1914		
Out-of- bounds Write	08-Sep-21	10	Possible buffer underflow due to lack of check for negative indices values when processing user provided input in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Voice & Music, Snapdragon Wearables CVE ID : CVE-2021-1916	https://www. qualcomm.co m/company/ product- security/bull etins/august- 2021-bulletin	H-QUA-SC81- 170921/1220
Integer Underflow (Wrap or Wraparoun d)	08-Sep-21	10	Integer underflow can occur when the RTCP length is lesser than than the actual blocks present in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Voice & Music, Snapdragon Wearables CVE ID : CVE-2021-1919	https://www. qualcomm.co m/company/ product- security/bull etins/august- 2021-bulletin	H-QUA-SC81- 170921/1221
Integer Underflow (Wrap or Wraparoun d)	08-Sep-21	10	Integer underflow can occur due to improper handling of incoming RTCP packets in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT,	https://www. qualcomm.co m/company/ product- security/bull etins/august- 2021-bulletin	H-QUA-SC81- 170921/1222

1-2

0-1

6-7

5-6

7-8

8-9

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Snapdragon IoT, Snapdragon Voice & Music, Snapdragon Wearables		
			CVE ID : CVE-2021-1920		
sd205					
Exposure of Resource to Wrong Sphere	08-Sep-21	2.1	Child process can leak information from parent process due to numeric pids are getting compared and these pid can be reused in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wearables CVE ID : CVE-2021-1904	https://www. qualcomm.co m/company/ product- security/bull etins/august- 2021-bulletin	H-QUA-SD20- 170921/1223
Loop with Unreachable Exit Condition ('Infinite Loop')	08-Sep-21	5	Loop with unreachable exit condition may occur due to improper handling of unsupported input in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Voice & Music, Snapdragon Wearables CVE ID : CVE-2021-1914	https://www. qualcomm.co m/company/ product- security/bull etins/august- 2021-bulletin	H-QUA-SD20- 170921/1224
Out-of- bounds Write	08-Sep-21	10	Possible buffer underflow due to lack of check for negative indices values when processing user provided input in Snapdragon Auto, Snapdragon Compute,	https://www. qualcomm.co m/company/ product- security/bull etins/august-	H-QUA-SD20- 170921/1225
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 & CVE ID	Patch	NCIIPC ID
			Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Voice & Music, Snapdragon Wearables	2021-bulletin	
			CVE ID : CVE-2021-1916		
Integer Underflow (Wrap or Wraparoun d)	08-Sep-21	10	Integer underflow can occur when the RTCP length is lesser than than the actual blocks present in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Voice & Music, Snapdragon Wearables	https://www. qualcomm.co m/company/ product- security/bull etins/august- 2021-bulletin	H-QUA-SD20- 170921/1226
			CVE ID : CVE-2021-1919		
Integer Underflow (Wrap or Wraparoun d)	08-Sep-21	10	Integer underflow can occur due to improper handling of incoming RTCP packets in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Voice & Music, Snapdragon Wearables CVE ID : CVE-2021-1920	https://www. qualcomm.co m/company/ product- security/bull etins/august- 2021-bulletin	H-QUA-SD20- 170921/1227
Out-of- bounds Read	08-Sep-21	3.6	Buffer over read could occur due to incorrect check of buffer size while flashing emmc devices in Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon	https://www. qualcomm.co m/company/ product- security/bull etins/august- 2021-bulletin	H-QUA-SD20- 170921/1228
CVSS Scoring Sca	ale 0-1	1-2	2-3 3-4 4-5 5-6	6-7 7-8	8-9 9-10

3-4 4-5 5-6 6-7 Page 437 of 1474

Weakness	Publish Date	CVSS	Description & CVE ID Patch		NCIIPC ID	
			Mobile, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking			
			CVE ID : CVE-2021-1928			
Exposure of Resource to Wrong Sphere	08-Sep-21	2.1	Lack of strict validation of bootmode can lead to information disclosure in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wearables CVE ID : CVE-2021-1929	https://www. qualcomm.co m/company/ product- security/bull etins/august- 2021-bulletin	H-QUA-SD20- 170921/1229	
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	08-Sep-21	10	Possible buffer overflow due to improper validation of device types during P2P search in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Woice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking CVE ID : CVE-2021-1972	https://www. qualcomm.co m/company/ product- security/bull etins/august- 2021-bulletin	H-QUA-SD20- 170921/1230	
sd210						
Exposure of Resource to Wrong Sphere	08-Sep-21	2.1	Child process can leak information from parent process due to numeric pids are getting compared and these pid can be reused in	https://www. qualcomm.co m/company/ product- security/bull	H-QUA-SD21- 170921/1231	
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 & CVE ID	Patch	NCIIPC ID
			Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables CVE ID : CVE-2021-1904	etins/august- 2021-bulletin	
Loop with Unreachable Exit Condition ('Infinite Loop')	08-Sep-21	5	Loop with unreachable exit condition may occur due to improper handling of unsupported input in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Voice & Music, Snapdragon Wearables CVE ID : CVE-2021-1914	https://www. qualcomm.co m/company/ product- security/bull etins/august- 2021-bulletin	H-QUA-SD21- 170921/1232
Out-of- bounds Write	08-Sep-21	10	Possible buffer underflow due to lack of check for negative indices values when processing user provided input in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Voice & Music, Snapdragon Wearables CVE ID : CVE-2021-1916	https://www. qualcomm.co m/company/ product- security/bull etins/august- 2021-bulletin	H-QUA-SD21- 170921/1233
Integer Underflow (Wrap or	08-Sep-21	10	Integer underflow can occur when the RTCP length is lesser than than the actual	https://www. qualcomm.co m/company/	H-QUA-SD21- 170921/1234

CVSS Scoring Scale	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10	
Page /39 of 1/17/											

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Wraparoun d)			blocks present in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Voice & Music, Snapdragon Wearables CVE ID : CVE-2021-1919	product- security/bull etins/august- 2021-bulletin	
Integer Underflow (Wrap or Wraparoun d)	08-Sep-21	10	Integer underflow can occur due to improper handling of incoming RTCP packets in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Voice & Music, Snapdragon Wearables CVE ID : CVE-2021-1920	https://www. qualcomm.co m/company/ product- security/bull etins/august- 2021-bulletin	H-QUA-SD21- 170921/1235
Out-of- bounds Read	08-Sep-21	3.6	Buffer over read could occur due to incorrect check of buffer size while flashing emmc devices in Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking CVE ID : CVE-2021-1928	https://www. qualcomm.co m/company/ product- security/bull etins/august- 2021-bulletin	H-QUA-SD21- 170921/1236
Exposure of Resource to Wrong Sphere	08-Sep-21	2.1	Lack of strict validation of bootmode can lead to information disclosure in Snapdragon Auto,	https://www. qualcomm.co m/company/ product-	H-QUA-SD21- 170921/1237
CVSS Scoring Sca	ale 0-1	1-2	2-3 3-4 4-5 5-6	6-7 7-8	8-9 9-10

Page 440 of 1474

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wearables	security/bull etins/august- 2021-bulletin	
			CVE ID : CVE-2021-1929		
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	08-Sep-21	10	Possible buffer overflow due to improper validation of device types during P2P search in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Woice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking CVE ID : CVE-2021-1972	https://www. qualcomm.co m/company/ product- security/bull etins/august- 2021-bulletin	H-QUA-SD21- 170921/1238
sd429	<u> </u>			<u> </u>	
Exposure of Resource to Wrong Sphere	08-Sep-21	2.1	Child process can leak information from parent process due to numeric pids are getting compared and these pid can be reused in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wearables CVE ID : CVE-2021-1904	https://www. qualcomm.co m/company/ product- security/bull etins/august- 2021-bulletin	H-QUA-SD42- 170921/1239

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID							
Unreachable Exit Condition ('Infinite Loop')			condition may occur due to improper handling of unsupported input in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Voice & Music, Snapdragon Wearables	qualcomm.co m/company/ product- security/bull etins/august- 2021-bulletin	170921/1240							
			CVE ID : CVE-2021-1914									
Out-of- bounds Write	08-Sep-21	10	Possible buffer underflow due to lack of check for negative indices values when processing user provided input in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Voice & Music, Snapdragon Wearables	https://www. qualcomm.co m/company/ product- security/bull etins/august- 2021-bulletin	H-QUA-SD42- 170921/1241							
Integer Underflow (Wrap or Wraparoun d)	08-Sep-21	10	CVE ID : CVE-2021-1916 Integer underflow can occur when the RTCP length is lesser than than the actual blocks present in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Voice & Music, Snapdragon Wearables CVE ID : CVE-2021-1919	https://www. qualcomm.co m/company/ product- security/bull etins/august- 2021-bulletin	H-QUA-SD42- 170921/1242							
Integer	08-Sep-21	10	Integer underflow can occur	https://www.	H-QUA-SD42-							
CVSS Scoring Sco	ale 0-1	1-2	2-3 3-4 4-5 5-6 Page 442 of 1474	6-7 7-8	CVSS Scoring Scale 0-1 1-2 2-3 3-4 4-5 5-6 6-7 7-8 8-9 9-10							

Page 442 of 1474

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Snapdragon Wearables		
			CVE ID : CVE-2021-1904		
Loop with Unreachable Exit Condition ('Infinite Loop')	08-Sep-21	5	Loop with unreachable exit condition may occur due to improper handling of unsupported input in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Voice & Music, Snapdragon Wearables	https://www. qualcomm.co m/company/ product- security/bull etins/august- 2021-bulletin	H-QUA-SD43- 170921/1246
			CVE ID : CVE-2021-1914		
Out-of- bounds Write	08-Sep-21	10	Possible buffer underflow due to lack of check for negative indices values when processing user provided input in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Voice & Music, Snapdragon Wearables CVE ID : CVE-2021-1916	https://www. qualcomm.co m/company/ product- security/bull etins/august- 2021-bulletin	H-QUA-SD43- 170921/1247
Integer Underflow (Wrap or Wraparoun d)	08-Sep-21	10	Integer underflow can occur when the RTCP length is lesser than than the actual blocks present in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Voice & Music, Snapdragon	https://www. qualcomm.co m/company/ product- security/bull etins/august- 2021-bulletin	H-QUA-SD43- 170921/1248

0-1

1-2

5-6

6-7

7-8

8-9

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Wearables		
			CVE ID : CVE-2021-1919		
Integer Underflow (Wrap or Wraparoun d)	08-Sep-21	10	Integer underflow can occur due to improper handling of incoming RTCP packets in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Voice & Music, Snapdragon Wearables	https://www. qualcomm.co m/company/ product- security/bull etins/august- 2021-bulletin	H-QUA-SD43- 170921/1249
			CVE ID : CVE-2021-1920		
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	08-Sep-21	10	Possible buffer overflow due to improper validation of device types during P2P search in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Woice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking CVE ID : CVE-2021-1972	https://www. qualcomm.co m/company/ product- security/bull etins/august- 2021-bulletin	H-QUA-SD43- 170921/1250
sd450				I	I
Exposure of Resource to Wrong Sphere	08-Sep-21	2.1	Child process can leak information from parent process due to numeric pids are getting compared and these pid can be reused in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity,	https://www. qualcomm.co m/company/ product- security/bull etins/august- 2021-bulletin	H-QUA-SD45- 170921/1251
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 & CVE ID	Patch	NCIIPC ID
			Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables CVE ID : CVE-2021-1904		
Loop with Unreachable Exit Condition ('Infinite Loop')	08-Sep-21	5	Loop with unreachable exit condition may occur due to improper handling of unsupported input in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Voice & Music, Snapdragon Wearables CVE ID : CVE-2021-1914	https://www. qualcomm.co m/company/ product- security/bull etins/august- 2021-bulletin	H-QUA-SD45- 170921/1252
Out-of- bounds Write	08-Sep-21	10	Possible buffer underflow due to lack of check for negative indices values when processing user provided input in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Voice & Music, Snapdragon Wearables CVE ID : CVE-2021-1916	https://www. qualcomm.co m/company/ product- security/bull etins/august- 2021-bulletin	H-QUA-SD45- 170921/1253
Integer Underflow (Wrap or Wraparoun d)	08-Sep-21	10	Integer underflow can occur when the RTCP length is lesser than than the actual blocks present in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity,	https://www. qualcomm.co m/company/ product- security/bull etins/august-	H-QUA-SD45- 170921/1254

0-1

2-3 3-4

1-2

4-5

5-6

6-7

7-8

8-9

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Voice & Music, Snapdragon Wearables CVE ID : CVE-2021-1919	2021-bulletin	
			Integer underflow can occur		
Integer Underflow (Wrap or Wraparoun d)	08-Sep-21	10	due to improper handling of incoming RTCP packets in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Voice & Music, Snapdragon Wearables	https://www. qualcomm.co m/company/ product- security/bull etins/august- 2021-bulletin	H-QUA-SD45- 170921/1255
			CVE ID : CVE-2021-1920		
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	08-Sep-21	10	Possible buffer overflow due to improper validation of device types during P2P search in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Woice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking CVE ID : CVE-2021-1972	https://www. qualcomm.co m/company/ product- security/bull etins/august- 2021-bulletin	H-QUA-SD45- 170921/1256
sd460					
Exposure of Resource to Wrong Sphere	08-Sep-21	2.1	Child process can leak information from parent process due to numeric pids are getting compared and	https://www. qualcomm.co m/company/ product-	H-QUA-SD46- 170921/1257
CVSS Scoring Sc	ale 0-1	1-2	2-3 3-4 4-5 5-6	6-7 7-8	8-9 9-10

Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
		these pid can be reused in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables CVE ID : CVE-2021-1904	security/bull etins/august- 2021-bulletin	
08-Sep-21	4.6	Incorrect pointer argument passed to trusted application TA could result in un- intended memory operations in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Industrial IOT CVE ID : CVE-2021-1923	https://www. qualcomm.co m/company/ product- security/bull etins/august- 2021-bulletin	H-QUA-SD46- 170921/1258
08-Sep-21	2.1	Lack of strict validation of bootmode can lead to information disclosure in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wearables CVE ID : CVE-2021-1929	https://www. qualcomm.co m/company/ product- security/bull etins/august- 2021-bulletin	H-QUA-SD46- 170921/1259
08-Sep-21	3.6	Possible out of bounds read due to incorrect validation of incoming buffer length in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT,	https://www. qualcomm.co m/company/ product- security/bull etins/august- 2021-bulletin	H-QUA-SD46- 170921/1260
	08-Sep-21	08-Sep-21 2.1 08-Sep-21 3.6	08-Sep-21Sanadragon Auto, Snapdragon Compute, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wearables08-Sep-214.64.6Incorrect pointer argument passed to trusted application TA could result in un- intended memory operations Snapdragon Compute, Snapdragon Compute, Snapdragon Industrial IOT08-Sep-214.64.6Incorrect pointer argument passed to trusted application TA could result in un- intended memory operations in Snapdragon Compute, Snapdragon Compute, Snapdragon Industrial IOT08-Sep-214.61Information disclosure in Snapdragon Compute, Snapdragon Compute, Snapdragon Compute, Snapdragon Muto, Snapdragon Industrial IOT Snapdragon Compute, Snapdragon Muto, Snapdragon Compute, Snapdragon Muto, Snapdragon Muto, Snapdragon Muto, Snapdragon Muto, Snapdragon Compute, Snapdragon Muto, Snapdragon Compute, Snapdragon Muto, Snapdragon Muto, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Mobile, Snapdragon Mobile, Snapdragon Mobile, Snapdragon Mobile, Snapdragon Muto, Snapdragon Mobile, Snapdragon Mobile, Snapdragon Mobile, Snapdragon Mobile, Snapdragon Mobile, Snapdragon Muto, Snapdragon Muto, <br< td=""><td>Image: series of the series</td></br<>	Image: series of the series

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Snapdragon Mobile		
			CVE ID : CVE-2021-1930		
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	08-Sep-21	10	Possible buffer overflow due to improper validation of device types during P2P search in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Woice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking CVE ID : CVE-2021-1972	https://www. qualcomm.co m/company/ product- security/bull etins/august- 2021-bulletin	H-QUA-SD46- 170921/1261
sd480					
Exposure of Resource to Wrong Sphere	08-Sep-21	2.1	Child process can leak information from parent process due to numeric pids are getting compared and these pid can be reused in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wearables CVE ID : CVE-2021-1904	https://www. qualcomm.co m/company/ product- security/bull etins/august- 2021-bulletin	H-QUA-SD48- 170921/1262
Loop with Unreachable Exit Condition ('Infinite Loop')	08-Sep-21	5	Loop with unreachable exit condition may occur due to improper handling of unsupported input in Snapdragon Auto, Snapdragon Compute,	https://www. qualcomm.co m/company/ product- security/bull etins/august-	H-QUA-SD48- 170921/1263
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 & CVE ID	Patch	NCIIPC ID
			Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Voice & Music, Snapdragon Wearables CVE ID : CVE-2021-1914	2021-bulletin	
Out-of- bounds Write	08-Sep-21	10	Possible buffer underflow due to lack of check for negative indices values when processing user provided input in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Voice & Music, Snapdragon Wearables CVE ID : CVE-2021-1916	https://www. qualcomm.co m/company/ product- security/bull etins/august- 2021-bulletin	H-QUA-SD48- 170921/1264
Integer Underflow (Wrap or Wraparoun d)	08-Sep-21	10	Integer underflow can occur when the RTCP length is lesser than than the actual blocks present in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Voice & Music, Snapdragon Wearables CVE ID : CVE-2021-1919	https://www. qualcomm.co m/company/ product- security/bull etins/august- 2021-bulletin	H-QUA-SD48- 170921/1265
Integer Underflow (Wrap or Wraparoun d)	08-Sep-21	10	Integer underflow can occur due to improper handling of incoming RTCP packets in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity,	https://www. qualcomm.co m/company/ product- security/bull etins/august-	H-QUA-SD48- 170921/1266

0-1

1-2

5-6

6-7

7-8

8-9

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Voice & Music, Snapdragon Wearables	2021-bulletin	
			CVE ID : CVE-2021-1920		
Incorrect Type Conversion or Cast	08-Sep-21	4.6	Incorrect pointer argument passed to trusted application TA could result in un- intended memory operations in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Industrial IOT	https://www. qualcomm.co m/company/ product- security/bull etins/august- 2021-bulletin	H-QUA-SD48- 170921/1267
			CVE ID : CVE-2021-1923		
Exposure of Resource to Wrong Sphere	08-Sep-21	2.1	Lack of strict validation of bootmode can lead to information disclosure in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wearables CVE ID : CVE-2021-1929	https://www. qualcomm.co m/company/ product- security/bull etins/august- 2021-bulletin	H-QUA-SD48- 170921/1268
Improper Restriction of Operations within the Bounds of a Memory Buffer	08-Sep-21	3.6	Possible out of bounds read due to incorrect validation of incoming buffer length in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile CVE ID : CVE-2021-1930	https://www. qualcomm.co m/company/ product- security/bull etins/august- 2021-bulletin	H-QUA-SD48- 170921/1269
Buffer Copy without CVSS Scoring Sco	08-Sep-21	10 1-2	Possible buffer overflow dueto improper validation of2-33-44-55-6	https://www. qualcomm.co	H-QUA-SD48-

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Checking Size of Input ('Classic Buffer Overflow')			device types during P2P search in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Woice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking CVE ID : CVE-2021-1972	m/company/ product- security/bull etins/august- 2021-bulletin	170921/1270
sd632					
Exposure of Resource to Wrong Sphere	08-Sep-21	2.1	Child process can leak information from parent process due to numeric pids are getting compared and these pid can be reused in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables CVE ID : CVE-2021-1904	https://www. qualcomm.co m/company/ product- security/bull etins/august- 2021-bulletin	H-QUA-SD63- 170921/1271
Loop with Unreachable Exit Condition ('Infinite Loop')	08-Sep-21	5	Loop with unreachable exit condition may occur due to improper handling of unsupported input in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Voice & Music, Snapdragon	https://www. qualcomm.co m/company/ product- security/bull etins/august- 2021-bulletin	H-QUA-SD63- 170921/1272

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Wearables		
			CVE ID : CVE-2021-1914		
Out-of- bounds Write	08-Sep-21	10	Possible buffer underflow due to lack of check for negative indices values when processing user provided input in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Voice & Music, Snapdragon Wearables	https://www. qualcomm.co m/company/ product- security/bull etins/august- 2021-bulletin	H-QUA-SD63- 170921/1273
			CVE ID : CVE-2021-1916		
Integer Underflow (Wrap or Wraparoun d)	08-Sep-21	10	Integer underflow can occur when the RTCP length is lesser than than the actual blocks present in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Voice & Music, Snapdragon Wearables CVE ID : CVE-2021-1919	https://www. qualcomm.co m/company/ product- security/bull etins/august- 2021-bulletin	H-QUA-SD63- 170921/1274
Integer Underflow (Wrap or Wraparoun d)	08-Sep-21	10	Integer underflow can occur due to improper handling of incoming RTCP packets in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Voice & Music, Snapdragon Wearables	https://www. qualcomm.co m/company/ product- security/bull etins/august- 2021-bulletin	H-QUA-SD63- 170921/1275
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 & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2021-1920		
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	08-Sep-21	10	Possible buffer overflow due to improper validation of device types during P2P search in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Woice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking CVE ID : CVE-2021-1972	https://www. qualcomm.co m/company/ product- security/bull etins/august- 2021-bulletin	H-QUA-SD63- 170921/1276
sd660					
Exposure of Resource to Wrong Sphere	08-Sep-21	2.1	Child process can leak information from parent process due to numeric pids are getting compared and these pid can be reused in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wearables CVE ID : CVE-2021-1904	https://www. qualcomm.co m/company/ product- security/bull etins/august- 2021-bulletin	H-QUA-SD66- 170921/1277
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	08-Sep-21	10	Possible buffer overflow due to improper validation of device types during P2P search in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT,	https://www. qualcomm.co m/company/ product- security/bull etins/august- 2021-bulletin	H-QUA-SD66- 170921/1278
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 & CVE ID	Patch	NCIIPC ID
			Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking		
sd662			CVE ID : CVE-2021-1972		
SU002					
Exposure of Resource to Wrong Sphere	08-Sep-21	2.1	Child process can leak information from parent process due to numeric pids are getting compared and these pid can be reused in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wearables CVE ID : CVE-2021-1904	https://www. qualcomm.co m/company/ product- security/bull etins/august- 2021-bulletin	H-QUA-SD66- 170921/1279
Incorrect Type Conversion or Cast	08-Sep-21	4.6	Incorrect pointer argument passed to trusted application TA could result in un- intended memory operations in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Industrial IOT CVE ID : CVE-2021-1923	https://www. qualcomm.co m/company/ product- security/bull etins/august- 2021-bulletin	H-QUA-SD66- 170921/1280
Exposure of Resource to Wrong Sphere	08-Sep-21	2.1	Lack of strict validation of bootmode can lead to information disclosure in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity,	https://www. qualcomm.co m/company/ product- security/bull etins/august-	H-QUA-SD66- 170921/1281
CVSS Scoring Sc	ale 0-1	1-2	2-3 3-4 4-5 5-6 Page 455 of 1474	6-7 7-8	8-9 9-10

Page 455 of 1474

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wearables	2021-bulletin	
			CVE ID : CVE-2021-1929		
Improper Restriction of Operations within the Bounds of a Memory Buffer	08-Sep-21	3.6	Possible out of bounds read due to incorrect validation of incoming buffer length in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile	https://www. qualcomm.co m/company/ product- security/bull etins/august- 2021-bulletin	H-QUA-SD66- 170921/1282
			CVE ID : CVE-2021-1930		
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	08-Sep-21	10	Possible buffer overflow due to improper validation of device types during P2P search in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Woice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking CVE ID : CVE-2021-1972	https://www. qualcomm.co m/company/ product- security/bull etins/august- 2021-bulletin	H-QUA-SD66- 170921/1283
sd665					
Exposure of Resource to Wrong Sphere	08-Sep-21	2.1	Child process can leak information from parent process due to numeric pids are getting compared and these pid can be reused in Snapdragon Auto, Snapdragon Compute,	https://www. qualcomm.co m/company/ product- security/bull etins/august- 2021-bulletin	H-QUA-SD66- 170921/1284
CVSS Scoring Sc	ale 0-1	1-2	2-3 3-4 4-5 5-6 Page 456 of 1474	6-7 7-8	8-9 9-10

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables		
			CVE ID : CVE-2021-1904		
Loop with Unreachable Exit Condition ('Infinite Loop')	08-Sep-21	5	Loop with unreachable exit condition may occur due to improper handling of unsupported input in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Voice & Music, Snapdragon Wearables	https://www. qualcomm.co m/company/ product- security/bull etins/august- 2021-bulletin	H-QUA-SD66- 170921/1285
			CVE ID : CVE-2021-1914		
Out-of- bounds Write	08-Sep-21	10	Possible buffer underflow due to lack of check for negative indices values when processing user provided input in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Voice & Music, Snapdragon Wearables CVE ID : CVE-2021-1916	https://www. qualcomm.co m/company/ product- security/bull etins/august- 2021-bulletin	H-QUA-SD66- 170921/1286
Integer Underflow (Wrap or Wraparoun d)	08-Sep-21	10	Integer underflow can occur when the RTCP length is lesser than than the actual blocks present in Snapdragon Auto, Snapdragon Compute,	https://www. qualcomm.co m/company/ product- security/bull	H-QUA-SD66- 170921/1287
CVSS Scoring Sca	ale 0-1	1-2	2-3 3-4 4-5 5-6	6-7 7-8	8-9 9-10

Page 457 of 1474

		Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Voice & Music, Snapdragon Wearables	etins/august- 2021-bulletin	
		CVE ID : CVE-2021-1919		
)8-Sep-21	10	Integer underflow can occur due to improper handling of incoming RTCP packets in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Voice & Music, Snapdragon Wearables	https://www. qualcomm.co m/company/ product- security/bull etins/august- 2021-bulletin	H-QUA-SD66- 170921/1288
		CVE ID : CVE-2021-1920		
)8-Sep-21	4.6	Incorrect pointer argument passed to trusted application TA could result in un- intended memory operations in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Industrial IOT CVE ID : CVE-2021-1923	https://www. qualcomm.co m/company/ product- security/bull etins/august- 2021-bulletin	H-QUA-SD66- 170921/1289
)8-Sep-21	2.1	Lack of strict validation of bootmode can lead to information disclosure in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wearables	https://www. qualcomm.co m/company/ product- security/bull etins/august- 2021-bulletin	H-QUA-SD66- 170921/1290
))	8-Sep-21	8-Sep-21 4.6 8-Sep-21 2.1	8-Sep-2110Snapdragon Compute, Snapdragon Connectivity, Snapdragon Industrial IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Voice & Music, Snapdragon Wearables8-Sep-214.6Incorrect pointer argument passed to trusted application TA could result in un- intended memory operations in Snapdragon Compute, Snapdragon Compute, Snapdragon Compute, Snapdragon Compute, Snapdragon Compute, Snapdragon Compute, Snapdragon Compute, Snapdragon Industrial IOT CVE ID : CVE-2021-19238-Sep-212.18-Sep-21Lack of strict validation of bootmode can lead to information disclosure in Snapdragon Compute, Snapdragon Industrial IOT, Snapdragon Industrial IOT, Snapdragon Consumer IOT, Snapdragon Mobile, Snapdragon Mobile, Snapdragon Mobile, Snapdragon Wearables	8-Sep-2110Snapdragon Compute, Snapdragon Connectivity, Snapdragon Iodustrial IOT, Snapdragon IoT, Snapdragon Voice & Music, Snapdragon Voice & Music, Snapdragon Wearablesqualcomm.co m/company/ product- security/bull etins/august- 2021-bulletin8-Sep-214.6Incorrect pointer argument passed to trusted application TA could result in un- intended memory operations in Snapdragon Compute, Snapdragon Industrial IOT CVE ID : CVE-2021-1920https://www. qualcomm.co m/company/ product- security/bull etins/august- 2021-bulletin8-Sep-214.6Incorrect pointer argument passed to trusted application TA could result in un- intended memory operations in Snapdragon Compute, Snapdragon Industrial IOT CVE ID : CVE-2021-1923https://www. qualcomm.co m/company/ product- security/bull etins/august- 2021-bulletin8-Sep-212.1Lack of strict validation of bootmode can lead to information disclosure in Snapdragon Connectivity, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Mobile,

 3-4
 4-5

 Page 458 of 1474

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2021-1929		
Improper Restriction of Operations within the Bounds of a Memory Buffer	08-Sep-21	3.6	Possible out of bounds read due to incorrect validation of incoming buffer length in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile CVE ID : CVE-2021-1930	https://www. qualcomm.co m/company/ product- security/bull etins/august- 2021-bulletin	H-QUA-SD66- 170921/1291
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	08-Sep-21	10	Possible buffer overflow due to improper validation of device types during P2P search in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Woice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking CVE ID : CVE-2021-1972	https://www. qualcomm.co m/company/ product- security/bull etins/august- 2021-bulletin	H-QUA-SD66- 170921/1292
sd670	I			I	
Exposure of Resource to Wrong Sphere	08-Sep-21	2.1	Child process can leak information from parent process due to numeric pids are getting compared and these pid can be reused in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile,	https://www. qualcomm.co m/company/ product- security/bull etins/august- 2021-bulletin	H-QUA-SD67- 170921/1293

1											
	CVSS Scoring Scale	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10
				D	200 450 0	f 1/7/					

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Snapdragon Voice & Music, Snapdragon Wearables		
			CVE ID : CVE-2021-1904		
Loop with Unreachable Exit Condition ('Infinite Loop')	08-Sep-21	5	Loop with unreachable exit condition may occur due to improper handling of unsupported input in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Voice & Music, Snapdragon Wearables CVE ID : CVE-2021-1914	https://www. qualcomm.co m/company/ product- security/bull etins/august- 2021-bulletin	H-QUA-SD67- 170921/1294
Out-of- bounds Write	08-Sep-21	10	Possible buffer underflow due to lack of check for negative indices values when processing user provided input in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Voice & Music, Snapdragon Wearables CVE ID : CVE-2021-1916	https://www. qualcomm.co m/company/ product- security/bull etins/august- 2021-bulletin	H-QUA-SD67- 170921/1295
Integer Underflow (Wrap or Wraparoun d)	08-Sep-21	10	Integer underflow can occur when the RTCP length is lesser than than the actual blocks present in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon	https://www. qualcomm.co m/company/ product- security/bull etins/august- 2021-bulletin	H-QUA-SD67- 170921/1296

1-2

0-1

5-6

6-7

7-8

8-9

Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
		Voice & Music, Snapdragon Wearables		
		CVE ID : CVE-2021-1919		
08-Sep-21	10	Integer underflow can occur due to improper handling of incoming RTCP packets in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Voice & Music, Snapdragon Wearables	https://www. qualcomm.co m/company/ product- security/bull etins/august- 2021-bulletin	H-QUA-SD67- 170921/1297
		CVE ID : CVE-2021-1920		
08-Sep-21	4.6	Incorrect pointer argument passed to trusted application TA could result in un- intended memory operations in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Industrial IOT CVE ID : CVE-2021-1923	https://www. qualcomm.co m/company/ product- security/bull etins/august- 2021-bulletin	H-QUA-SD67- 170921/1298
08-Sep-21	3.6	Possible out of bounds read due to incorrect validation of incoming buffer length in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile CVE ID : CVE-2021-1930	https://www. qualcomm.co m/company/ product- security/bull etins/august- 2021-bulletin	H-QUA-SD67- 170921/1299
08-Sep-21	10	Possible buffer overflow due to improper validation of device types during P2P search in Snapdragon Auto,	https://www. qualcomm.co m/company/ product-	H-QUA-SD67- 170921/1300
	08-Sep-21 08-Sep-21 08-Sep-21	No No No No	Image: constraint of the second sec	Image: Note of the second se

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
('Classic Buffer Overflow')			Snapdragon Compute,security/bullSnapdragon Connectivity,etins/august-Snapdragon Consumer IOT,2021-bulletinSnapdragon Industrial IOT,Snapdragon Mobile,Snapdragon Voice & Music,Snapdragon Wearables,Snapdragon WiredInfrastructure andNetworkingCVE ID : CVE-2021-1972		
sd675					
Exposure of Resource to Wrong Sphere	08-Sep-21	2.1	Child process can leak information from parent process due to numeric pids are getting compared and these pid can be reused in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables CVE ID : CVE-2021-1904	https://www. qualcomm.co m/company/ product- security/bull etins/august- 2021-bulletin	H-QUA-SD67- 170921/1301
Loop with Unreachable Exit Condition ('Infinite Loop')	08-Sep-21	5	Loop with unreachable exit condition may occur due to improper handling of unsupported input in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Voice & Music, Snapdragon Wearables	https://www. qualcomm.co m/company/ product- security/bull etins/august- 2021-bulletin	H-QUA-SD67- 170921/1302

CVSS	Scoring	Scale
0.00	2001112	ocure

0-1

1-2

6-7

5-6

7-8

8-9

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2021-1914		
Out-of- bounds Write	08-Sep-21	10	Possible buffer underflow due to lack of check for negative indices values when processing user provided input in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Voice & Music, Snapdragon Wearables CVE ID : CVE-2021-1916	https://www. qualcomm.co m/company/ product- security/bull etins/august- 2021-bulletin	H-QUA-SD67- 170921/1303
Integer Underflow (Wrap or Wraparoun d)	08-Sep-21	10	Integer underflow can occur when the RTCP length is lesser than than the actual blocks present in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Voice & Music, Snapdragon Wearables CVE ID : CVE-2021-1919	https://www. qualcomm.co m/company/ product- security/bull etins/august- 2021-bulletin	H-QUA-SD67- 170921/1304
Integer Underflow (Wrap or Wraparoun d)	08-Sep-21	10	Integer underflow can occur due to improper handling of incoming RTCP packets in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Voice & Music, Snapdragon Wearables CVE ID : CVE-2021-1920	https://www. qualcomm.co m/company/ product- security/bull etins/august- 2021-bulletin	H-QUA-SD67- 170921/1305
CVSS Scoring Sc	ale 0-1	1-2	2-3 3-4 4-5 5-6 Page 463 of 1474	6-7 7-8	8-9 9-10

Page 463 of 1474

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Incorrect Type Conversion or Cast	08-Sep-21	4.6	Incorrect pointer argument passed to trusted application TA could result in un- intended memory operations in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Industrial IOT CVE ID : CVE-2021-1923	https://www. qualcomm.co m/company/ product- security/bull etins/august- 2021-bulletin	H-QUA-SD67- 170921/1306
Exposure of Resource to Wrong Sphere	08-Sep-21	2.1	Lack of strict validation of bootmode can lead to information disclosure in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wearables CVE ID : CVE-2021-1929	https://www. qualcomm.co m/company/ product- security/bull etins/august- 2021-bulletin	H-QUA-SD67- 170921/1307
Improper Restriction of Operations within the Bounds of a Memory Buffer	08-Sep-21	3.6	Possible out of bounds read due to incorrect validation of incoming buffer length in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile CVE ID : CVE-2021-1930	https://www. qualcomm.co m/company/ product- security/bull etins/august- 2021-bulletin	H-QUA-SD67- 170921/1308
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	08-Sep-21	10	Possible buffer overflow due to improper validation of device types during P2P search in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT,	https://www. qualcomm.co m/company/ product- security/bull etins/august- 2021-bulletin	H-QUA-SD67- 170921/1309

0-1

1-2

5-6

6-7

7-8

8-9

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking		
			CVE ID : CVE-2021-1972		
sd678				I	I
Exposure of Resource to Wrong Sphere	08-Sep-21	2.1	Child process can leak information from parent process due to numeric pids are getting compared and these pid can be reused in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wearables CVE ID : CVE-2021-1904	https://www. qualcomm.co m/company/ product- security/bull etins/august- 2021-bulletin	H-QUA-SD67- 170921/1310
Loop with Unreachable Exit Condition ('Infinite Loop')	08-Sep-21	5	Loop with unreachable exit condition may occur due to improper handling of unsupported input in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Voice & Music, Snapdragon Wearables CVE ID : CVE-2021-1914	https://www. qualcomm.co m/company/ product- security/bull etins/august- 2021-bulletin	H-QUA-SD67- 170921/1311
Out-of- bounds Write	08-Sep-21	10	Possible buffer underflow due to lack of check for negative indices values when	https://www. qualcomm.co m/company/	H-QUA-SD67- 170921/1312

Page 465 of 1474

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID	
			processing user provided input in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Voice & Music, Snapdragon Wearables CVE ID : CVE-2021-1916	product- security/bull etins/august- 2021-bulletin		
Integer Underflow (Wrap or Wraparoun d)	08-Sep-21	10	Integer underflow can occur when the RTCP length is lesser than than the actual blocks present in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Voice & Music, Snapdragon Wearables CVE ID : CVE-2021-1919	https://www. qualcomm.co m/company/ product- security/bull etins/august- 2021-bulletin	H-QUA-SD67- 170921/1313	
Integer Underflow (Wrap or Wraparoun d)	08-Sep-21	10	Integer underflow can occur due to improper handling of incoming RTCP packets in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Voice & Music, Snapdragon Wearables CVE ID : CVE-2021-1920	https://www. qualcomm.co m/company/ product- security/bull etins/august- 2021-bulletin	H-QUA-SD67- 170921/1314	
Incorrect Type Conversion or Cast	08-Sep-21	4.6	Incorrect pointer argument passed to trusted application TA could result in un- intended memory operations	https://www. qualcomm.co m/company/ product-	H-QUA-SD67- 170921/1315	
CVSS Scoring Scale 0-1 1-2 2-3 3-4 4-5 5-6 6-7 7-8 8-9 9-10 Page 466 of 1474						

Page 466 of 1474

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Industrial IOT CVE ID : CVE-2021-1923	security/bull etins/august- 2021-bulletin	
Exposure of Resource to Wrong Sphere	08-Sep-21	2.1	Lack of strict validation of bootmode can lead to information disclosure in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wearables CVE ID : CVE-2021-1929	https://www. qualcomm.co m/company/ product- security/bull etins/august- 2021-bulletin	H-QUA-SD67- 170921/1316
Improper Restriction of Operations within the Bounds of a Memory Buffer	08-Sep-21	3.6	Possible out of bounds read due to incorrect validation of incoming buffer length in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile CVE ID : CVE-2021-1930	https://www. qualcomm.co m/company/ product- security/bull etins/august- 2021-bulletin	H-QUA-SD67- 170921/1317
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	08-Sep-21	10	Possible buffer overflow due to improper validation of device types during P2P search in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Woice & Music, Snapdragon Wearables, Snapdragon Wired	https://www. qualcomm.co m/company/ product- security/bull etins/august- 2021-bulletin	H-QUA-SD67- 170921/1318

0-1

1-2

5-6

6-7

7-8

8-9

		Infrastructure and Networking							
		0							
		CVE ID : CVE-2021-1972							
sd690_5g									
08-Sep-21	2.1	information from parent process due to numeric pids are getting compared and these pid can be reused in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wearables	https://www. qualcomm.co m/company/ product- security/bull etins/august- 2021-bulletin	H-QUA-SD69- 170921/1319					
08-Sep-21	5	Loop with unreachable exit condition may occur due to improper handling of unsupported input in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Voice & Music, Snapdragon Wearables CVE ID : CVE-2021-1914	https://www. qualcomm.co m/company/ product- security/bull etins/august- 2021-bulletin	H-QUA-SD69- 170921/1320					
		Possible buffer underflow	https://www.						
08-Sep-21	10	due to lack of check for negative indices values when processing user provided input in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity,	qualcomm.co m/company/ product- security/bull etins/august- 2021-bulletin	H-QUA-SD69- 170921/1321					
	08-Sep-21	08-Sep-212.1process due to numeric pids are getting compared and these pid can be reused in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer IOT, Snapdragon Mobile, Snapdragon Wearables08-Sep-212.1CVE ID: CVE-2021-190408-Sep-215Loop with unreachable exit condition may occur due to improper handling of unsupported input in Snapdragon Consumer IOT, Snapdragon Wearables08-Sep-215Loop with unreachable exit condition may occur due to improper handling of unsupported input in Snapdragon Compute, Snapdragon Consumer IOT, Snapdragon Consumer IOT, Snapdragon Compute, Snapdragon Industrial IOT, Snapdragon Industrial IOT, SnapdragonI	08-Sep-211Child process can leak information from parent process due to numeric pids are getting compared and these pid can be reused in Snapdragon Auto, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Nobile, Snapdragon Nobile, Snapdragon Voice & Music, Snapdragon Consumer IOT, Snapdragon Voice & Music, Snapdragon Connectivity, Snapdragon Connectivity, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Compute, Snapdragon Industrial IOT, Snapdragon Industrial IOT, Snapdragon Connectivity, Snapdragon Industrial IOT, Snapdragon Iot, Snapdragon Voice & Music, Snapdragon Compute, Snapdragon Compute, Snapdragon Compute, Snapdragon Compute, Snapdragon Compute, Snapdragon Compute, Snapdragon Compute, Snapdragon Compute, Snapdragon Compute, Sna					

		Description & CVE ID	Patch	NCIIPC ID
		Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Voice & Music, Snapdragon Wearables		
08-Sep-21	10	Integer undernow can occur when the RTCP length is lesser than than the actual blocks present in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Voice & Music, Snapdragon Wearables	https://www. qualcomm.co m/company/ product- security/bull etins/august- 2021-bulletin	H-QUA-SD69- 170921/1322
		CVE ID : CVE-2021-1919		
08-Sep-21	10	Integer underflow can occur due to improper handling of incoming RTCP packets in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Voice & Music, Snapdragon Wearables	https://www. qualcomm.co m/company/ product- security/bull etins/august- 2021-bulletin	H-QUA-SD69- 170921/1323
		CVE ID : CVE-2021-1920		
08-Sep-21	4.6	Incorrect pointer argument passed to trusted application TA could result in un- intended memory operations in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Industrial IOT	https://www. qualcomm.co m/company/ product- security/bull etins/august- 2021-bulletin	H-QUA-SD69- 170921/1324
	08-Sep-21	08-Sep-21 10	Note: Substrain the sector of the sector o	Napdragon Industrial IOT, Snapdragon IoT, Snapdragon Voice & Music, Snapdragon WearablesInteger underflow can occur when the RTCP length is lesser than than the actual blocks present in Snapdragon Auto, Snapdragon Compute, Snapdragon Industrial IOT, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Industrial IOT, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Compute, Snapdragon Compute, Snapdragon Compute, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Voice & Music, Sna

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2021-1923		
Improper Restriction of Operations within the Bounds of a Memory Buffer	08-Sep-21	3.6	Possible out of bounds read due to incorrect validation of incoming buffer length in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile CVE ID : CVE-2021-1930	https://www. qualcomm.co m/company/ product- security/bull etins/august- 2021-bulletin	H-QUA-SD69- 170921/1325
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	08-Sep-21	10	Possible buffer overflow due to improper validation of device types during P2P search in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Woice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking CVE ID : CVE-2021-1972	https://www. qualcomm.co m/company/ product- security/bull etins/august- 2021-bulletin	H-QUA-SD69- 170921/1326
sd710	I			I	
Exposure of Resource to Wrong Sphere	08-Sep-21	2.1	Child process can leak information from parent process due to numeric pids are getting compared and these pid can be reused in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile,	https://www. qualcomm.co m/company/ product- security/bull etins/august- 2021-bulletin	H-QUA-SD71- 170921/1327

CVSS Scoring Scale	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10
			D	200 170 0	f 1/7/					

		Snapdragon Voice & Music, Snapdragon Wearables CVE ID : CVE-2021-1904		
08-Sep-21	3.6	Possible out of bounds read due to incorrect validation of incoming buffer length in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile CVE ID : CVE-2021-1930	https://www. qualcomm.co m/company/ product- security/bull etins/august- 2021-bulletin	H-QUA-SD71- 170921/1328
08-Sep-21	10	Possible buffer overflow due to improper validation of device types during P2P search in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Woice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking CVE ID : CVE-2021-1972	https://www. qualcomm.co m/company/ product- security/bull etins/august- 2021-bulletin	H-QUA-SD71- 170921/1329
08-Sep-21	5	Loop with unreachable exit condition may occur due to improper handling of unsupported input in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT,	https://www. qualcomm.co m/company/ product- security/bull etins/august- 2021-bulletin	H-QUA-SD71- 170921/1330
	08-Sep-21		Note08-Sep-21CVE ID : CVE-2021-190408-Sep-21Possible out of bounds read due to incorrect validation of incoming buffer length in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon MobileVEVE ID : CVE-2021-1930CVE ID : CVE-2021-193008-Sep-21Possible buffer overflow due to improper validation of device types during P2P search in Snapdragon Consumer IOT, Snapdragon Compute, Snapdragon Compute, Snapdragon Compute, Snapdragon Consumer IOT, Snapdragon Consumer IOT, Snapdragon Consumer IOT, Snapdragon Consumer IOT, Snapdragon Consumer IOT, Snapdragon Consumer IOT, Snapdragon Mobile, Snapdragon Mobile, Snapdragon Mobile, Snapdragon Wierd Infrastructure and Networking08-Sep-21Ever ID : CVE-2021-197208-Sep-21Ever ID : CVE-2021-197208-Sep-21Sapdragon Mired Infrastructure and Networking08-Sep-21For With unreachable exit Condition may occur due to improper handling of unsupported input in Snapdragon Compute, Snapdragon Compute, Snapdragon Compute, Snapdragon Auto, Snapdragon Compute, Snapdragon	OB-Sep-21CVE ID:CVF-2021-1904Https://www. qualcomm.co08-Sep-213.6Possible out of bounds read due to incorrect validation of Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Mobilehttps://www. qualcomm.co m/company/ product- security/bull etins/august- 2021-bulletin08-Sep-2110Possible buffer overflow due to improper validation of device types during P2P search in Snapdragon Connectivity, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Consumer IOT, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Mobilehttps://www. qualcomm.co m/company/ product- security/bull etins/august- 2021-bulletin08-Sep-2110Snapdragon Mobile, Snapdragon Mobile, Snapdragon Nobile, Snapdragon Wired Infrastructure and Networking CVE ID: CVE-2021-1972https://www. qualcomm.co m/company/ product- security/bull etins/august- 2021-bulletin08-Sep-215Loop with unreachable exit condition may occur due to improper handling of unsuported input in Snapdragon Connectivity, Snapdragon Conne

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Snapdragon IoT, Snapdragon Voice & Music, Snapdragon Wearables		
			CVE ID : CVE-2021-1914		
Out-of- bounds Write	08-Sep-21	10	Possible buffer underflow due to lack of check for negative indices values when processing user provided input in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Voice & Music, Snapdragon Wearables	https://www. qualcomm.co m/company/ product- security/bull etins/august- 2021-bulletin	H-QUA-SD71- 170921/1331
			CVE ID : CVE-2021-1916 Integer underflow can occur		
Integer Underflow (Wrap or Wraparoun d)	08-Sep-21	10	when the RTCP length is lesser than than the actual blocks present in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Voice & Music, Snapdragon Wearables	https://www. qualcomm.co m/company/ product- security/bull etins/august- 2021-bulletin	H-QUA-SD71- 170921/1332
			CVE ID : CVE-2021-1919		
Integer Underflow (Wrap or Wraparoun d)	08-Sep-21	10	Integer underflow can occur due to improper handling of incoming RTCP packets in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon	https://www. qualcomm.co m/company/ product- security/bull etins/august- 2021-bulletin	H-QUA-SD71- 170921/1333

1-2

0-1

6-7

5-6

7-8

8-9

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Voice & Music, Snapdragon Wearables		
			CVE ID : CVE-2021-1920		
sd720g					
Exposure of Resource to Wrong Sphere	08-Sep-21	2.1	Child process can leak information from parent process due to numeric pids are getting compared and these pid can be reused in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wearables CVE ID : CVE-2021-1904	https://www. qualcomm.co m/company/ product- security/bull etins/august- 2021-bulletin	H-QUA-SD72- 170921/1334
Loop with Unreachable Exit Condition ('Infinite Loop')	08-Sep-21	5	Loop with unreachable exit condition may occur due to improper handling of unsupported input in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Voice & Music, Snapdragon Wearables CVE ID : CVE-2021-1914	https://www. qualcomm.co m/company/ product- security/bull etins/august- 2021-bulletin	H-QUA-SD72- 170921/1335
Out-of- bounds Write	08-Sep-21	10	Possible buffer underflow due to lack of check for negative indices values when processing user provided input in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity,	https://www. qualcomm.co m/company/ product- security/bull etins/august- 2021-bulletin	H-QUA-SD72- 170921/1336

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Voice & Music, Snapdragon Wearables CVE ID : CVE-2021-1916		
Integer Underflow (Wrap or Wraparoun d)	08-Sep-21	10	Integer underflow can occur when the RTCP length is lesser than than the actual blocks present in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Voice & Music, Snapdragon Wearables	https://www. qualcomm.co m/company/ product- security/bull etins/august- 2021-bulletin	H-QUA-SD72- 170921/1337
Integer Underflow (Wrap or Wraparoun d)	08-Sep-21	10	CVE ID : CVE-2021-1919 Integer underflow can occur due to improper handling of incoming RTCP packets in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Voice & Music, Snapdragon Wearables CVE ID : CVE-2021-1920	https://www. qualcomm.co m/company/ product- security/bull etins/august- 2021-bulletin	H-QUA-SD72- 170921/1338
Incorrect Type Conversion or Cast	08-Sep-21	4.6	Incorrect pointer argument passed to trusted application TA could result in un- intended memory operations in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Industrial IOT	https://www. qualcomm.co m/company/ product- security/bull etins/august- 2021-bulletin	H-QUA-SD72- 170921/1339
CVSS Scoring Sc	ale 0-1	1-2	2-3 3-4 4-5 5-6	6-7 7-8	8-9 9-10

 3-4
 4-5
 5-6

 Page 474 of 1474

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2021-1923		
Exposure of Resource to Wrong Sphere	08-Sep-21	2.1	Lack of strict validation of bootmode can lead to information disclosure in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wearables CVE ID : CVE-2021-1929	https://www. qualcomm.co m/company/ product- security/bull etins/august- 2021-bulletin	H-QUA-SD72- 170921/1340
Improper Restriction of Operations within the Bounds of a Memory Buffer	08-Sep-21	3.6	Possible out of bounds read due to incorrect validation of incoming buffer length in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile CVE ID : CVE-2021-1930	https://www. qualcomm.co m/company/ product- security/bull etins/august- 2021-bulletin	H-QUA-SD72- 170921/1341
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	08-Sep-21	10	Possible buffer overflow due to improper validation of device types during P2P search in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Industrial IOT, Snapdragon Woile, Snapdragon Woice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking CVE ID : CVE-2021-1972	https://www. qualcomm.co m/company/ product- security/bull etins/august- 2021-bulletin	H-QUA-SD72- 170921/1342
sd730					
CVSS Scoring Sc	ale 0-1	1-2	2-3 3-4 4-5 5-6	6-7 7-8	8-9 9-10

Exposure of Resource to Wrong Sphere08-Sep-21Z.1Child process can leak information from parent process due to numeric pids are getting compared and these pid can be reused in Snapdragon Conneutivity, Snapdragon Consumer 10T, Snapdragon Consumer 10T, Snapdragon Onubet, Snapdragon Onubet, Snapdragon Consumer 10T, Snapdragon Onubet, Snapdragon Onuetration Snapdragon Consumer 10T, Snapdragon Voice & Music, Snapdragon Wearableshttps://www. qualcomm.co m/company/ product- security/bull etins/august- 2021/bulletinH-QUA-SD73- 170921/1343Loop with Unreachable Exit Condition ('Infinite Loop')08-Sep-215Songdragon Consumer 10T, Snapdragon Muto, Snapdragon Consumer 10T, Snapdragon Industrial 10T, Snapdragon Consumer 10T, Snapdragon Consumer 10T, Snapdragon Industrial 10T, Snapdragon Industrial 10T, Snapdragon Industrial 10T, Snapdragon Consumer 10T, Snapdragon Consumer 10T, Snapdragon Industrial 10T, Snapdragon Consumer 10T, Snap	Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Loop with Unreachable Exit Condition ('Infinite Loop')08-Sep-215condition may occur due to improper handling of unsupported input in Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon WearablesH-QUA-SD73- IT0921/1344Out-of- bounds Write08-Sep-2110Possible buffer underflow due to lack of check for negative indices values when processing user provided input in Snapdragon Compute, Snapdragon Consumer IOT, Snapdragon Consumer IOT, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Consumer IOT, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Industrial IOT, Snapdragon Industrial IOT, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Sonadragon Industrial IOT, S	Resource to Wrong	08-Sep-21	2.1	information from parent process due to numeric pids are getting compared and these pid can be reused in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wearables	qualcomm.co m/company/ product- security/bull etins/august-	•
Out-of- bounds08-Sep-2110Image: Constraint of the const	Unreachable Exit Condition ('Infinite	08-Sep-21	5	condition may occur due to improper handling of unsupported input in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Voice & Music, Snapdragon Wearables	qualcomm.co m/company/ product- security/bull etins/august-	e e
	bounds	08-Sep-21	10	due to lack of check for negative indices values when processing user provided input in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Voice & Music, Snapdragon	qualcomm.co m/company/ product- security/bull etins/august-	•

Page 476 of 1474

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2021-1916		
Integer Underflow (Wrap or Wraparoun d)	08-Sep-21	10	Integer underflow can occur when the RTCP length is lesser than than the actual blocks present in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Voice & Music, Snapdragon Wearables CVE ID : CVE-2021-1919	https://www. qualcomm.co m/company/ product- security/bull etins/august- 2021-bulletin	H-QUA-SD73- 170921/1346
Integer Underflow (Wrap or Wraparoun d)	08-Sep-21	10	Integer underflow can occur due to improper handling of incoming RTCP packets in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Voice & Music, Snapdragon Wearables CVE ID : CVE-2021-1920	https://www. qualcomm.co m/company/ product- security/bull etins/august- 2021-bulletin	H-QUA-SD73- 170921/1347
Incorrect Type Conversion or Cast	08-Sep-21	4.6	Incorrect pointer argument passed to trusted application TA could result in un- intended memory operations in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Industrial IOT CVE ID : CVE-2021-1923	https://www. qualcomm.co m/company/ product- security/bull etins/august- 2021-bulletin	H-QUA-SD73- 170921/1348
Exposure of Resource to Wrong Sphere CVSS Scoring Sc	08-Sep-21 ale 0-1	2.1	Lack of strict validation of bootmode can lead to information disclosure in Snapdragon Auto, 2-3 3-4 4-5 5-6	https://www. qualcomm.co m/company/ product-	H-QUA-SD73- 170921/1349 8-9 9-10

Page 477 of 1474

p-21 3	8.6	Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wearables CVE ID : CVE-2021-1929 Possible out of bounds read due to incorrect validation of incoming buffer length in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Industrial IOT, Snapdragon Industrial IOT, Snapdragon Mobile CVE ID : CVE-2021-1930 Possible buffer overflow due	security/bull etins/august- 2021-bulletin https://www. qualcomm.co m/company/ product- security/bull etins/august- 2021-bulletin	H-QUA-SD73- 170921/1350
p-21 3	8.6	Possible out of bounds read due to incorrect validation of incoming buffer length in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile CVE ID : CVE-2021-1930 Possible buffer overflow due	qualcomm.co m/company/ product- security/bull etins/august-	e e
p-21 3	3.6	due to incorrect validation of incoming buffer length in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile CVE ID : CVE-2021-1930 Possible buffer overflow due	qualcomm.co m/company/ product- security/bull etins/august-	e e
p-21 1	.0	to improper validation of device types during P2P search in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Woice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking CVE ID : CVE-2021-1972	https://www. qualcomm.co m/company/ product- security/bull etins/august- 2021-bulletin	H-QUA-SD73- 170921/1351
	2.1	Child process can leak information from parent process due to numeric pids	https://www. qualcomm.co m/company/ product-	H-QUA-SD75- 170921/1352
	p-21 2	p-21 2.1	Networking CVE ID : CVE-2021-1972 Child process can leak information from parent	p-21 2.1 Networking CVE ID : CVE-2021-1972 Child process can leak information from parent process due to numeric pids Metworking https://www. qualcomm.co m/company/

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables CVE ID : CVE-2021-1904	etins/august- 2021-bulletin	
Loop with Unreachable Exit Condition ('Infinite Loop')	08-Sep-21	5	Loop with unreachable exit condition may occur due to improper handling of unsupported input in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Voice & Music, Snapdragon Wearables CVE ID : CVE-2021-1914	https://www. qualcomm.co m/company/ product- security/bull etins/august- 2021-bulletin	H-QUA-SD75- 170921/1353
Out-of- bounds Write	08-Sep-21	10	Possible buffer underflow due to lack of check for negative indices values when processing user provided input in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Voice & Music, Snapdragon Wearables CVE ID : CVE-2021-1916	https://www. qualcomm.co m/company/ product- security/bull etins/august- 2021-bulletin	H-QUA-SD75- 170921/1354
Integer Underflow (Wrap or	08-Sep-21	10	Integer underflow can occur when the RTCP length is lesser than than the actual	https://www. qualcomm.co m/company/	H-QUA-SD75- 170921/1355

CVSS Scoring Scale	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10
		•	D	200 170 0	f 1/7/					

Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
		blocks present in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Voice & Music, Snapdragon Wearables CVE ID : CVE-2021-1919	product- security/bull etins/august- 2021-bulletin	
08-Sep-21	10	Integer underflow can occur due to improper handling of incoming RTCP packets in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Voice & Music, Snapdragon Wearables CVE ID : CVE-2021-1920	https://www. qualcomm.co m/company/ product- security/bull etins/august- 2021-bulletin	H-QUA-SD75- 170921/1356
08-Sep-21	4.6	Incorrect pointer argument passed to trusted application TA could result in un- intended memory operations in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Industrial IOT CVE ID : CVE-2021-1923	https://www. qualcomm.co m/company/ product- security/bull etins/august- 2021-bulletin	H-QUA-SD75- 170921/1357
08-Sep-21	3.6	Possible out of bounds read due to incorrect validation of incoming buffer length in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT,	https://www. qualcomm.co m/company/ product- security/bull etins/august- 2021-bulletin	H-QUA-SD75- 170921/1358
	08-Sep-21 08-Sep-21	08-Sep-21 10 08-Sep-21 4.6 08-Sep-21 4.6	Image: construct of the second seco	08-Sep-21110Incress products products products security/bull sinapdragon Compute, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Voice & Music, Snapdragon Voice & Music, Snapdragon Voice & Music, Snapdragon Voice & Music, Snapdragon Compute, Snapdragon Auto, Snapdragon Connectivity, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Connectivity, Snapdragon Industrial IOT, Snapdragon Industrial IOT, Snapdragon Connectivity, Snapdragon Connectivity, Snapdragon Industrial IOT, Snapdragon Connectivity, Snapdragon Connectivity, Snapdragon Connectivity, Snapdragon Connectivity, Snapdragon Industrial IOThttps://www.qualcomm.co08-Sep-214.6Possible out of bounds read due to incorrect validation of incoming buffer length in Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon

			Description & CVE ID Patch		NCIIPC ID
			Snapdragon Mobile		
			CVE ID : CVE-2021-1930		
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	08-Sep-21	10	Possible buffer overflow due to improper validation of device types during P2P search in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Woice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking CVE ID : CVE-2021-1972	https://www. qualcomm.co m/company/ product- security/bull etins/august- 2021-bulletin	H-QUA-SD75- 170921/1359
sd765					
Exposure of Resource to Wrong Sphere	08-Sep-21	2.1	Child process can leak information from parent process due to numeric pids are getting compared and these pid can be reused in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wearables CVE ID : CVE-2021-1904	https://www. qualcomm.co m/company/ product- security/bull etins/august- 2021-bulletin	H-QUA-SD76- 170921/1360
Loop with Unreachable Exit Condition ('Infinite Loop')	08-Sep-21	5	Loop with unreachable exit condition may occur due to improper handling of unsupported input in Snapdragon Auto, Snapdragon Compute,	https://www. qualcomm.co m/company/ product- security/bull etins/august-	H-QUA-SD76- 170921/1361

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Voice & Music, Snapdragon Wearables CVE ID : CVE-2021-1914	2021-bulletin	
Out-of- bounds Write	08-Sep-21	10	Possible buffer underflow due to lack of check for negative indices values when processing user provided input in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Voice & Music, Snapdragon Wearables CVE ID : CVE-2021-1916	https://www. qualcomm.co m/company/ product- security/bull etins/august- 2021-bulletin	H-QUA-SD76- 170921/1362
Integer Underflow (Wrap or Wraparoun d)	08-Sep-21	10	Integer underflow can occur when the RTCP length is lesser than than the actual blocks present in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Voice & Music, Snapdragon Wearables CVE ID : CVE-2021-1919	https://www. qualcomm.co m/company/ product- security/bull etins/august- 2021-bulletin	H-QUA-SD76- 170921/1363
Integer Underflow (Wrap or Wraparoun d)	08-Sep-21	10	Integer underflow can occur due to improper handling of incoming RTCP packets in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity,	https://www. qualcomm.co m/company/ product- security/bull etins/august-	H-QUA-SD76- 170921/1364

0-1

1-2

5-6

6-7

7-8

8-9

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Voice & Music, Snapdragon Wearables CVE ID : CVE-2021-1920	2021-bulletin	
Incorrect Type Conversion or Cast	08-Sep-21	4.6	Incorrect pointer argument passed to trusted application TA could result in un- intended memory operations in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Industrial IOT	https://www. qualcomm.co m/company/ product- security/bull etins/august- 2021-bulletin	H-QUA-SD76- 170921/1365
			CVE ID : CVE-2021-1923		
Exposure of Resource to Wrong Sphere	08-Sep-21	2.1	Lack of strict validation of bootmode can lead to information disclosure in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wearables CVE ID : CVE-2021-1929	https://www. qualcomm.co m/company/ product- security/bull etins/august- 2021-bulletin	H-QUA-SD76- 170921/1366
Improper Restriction of Operations within the Bounds of a Memory Buffer	08-Sep-21	3.6	Possible out of bounds read due to incorrect validation of incoming buffer length in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile CVE ID : CVE-2021-1930	https://www. qualcomm.co m/company/ product- security/bull etins/august- 2021-bulletin	H-QUA-SD76- 170921/1367
Buffer Copy without CVSS Scoring Sc	08-Sep-21	10 1-2	Possible buffer overflow dueto improper validation of2-33-44-55-6	https://www. qualcomm.co	H-QUA-SD76-

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Checking Size of Input ('Classic Buffer Overflow')			device types during P2P search in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Woice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking CVE ID : CVE-2021-1972	m/company/ product- security/bull etins/august- 2021-bulletin	170921/1368
sd765g					
Exposure of Resource to Wrong Sphere	08-Sep-21	2.1	Child process can leak information from parent process due to numeric pids are getting compared and these pid can be reused in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables CVE ID : CVE-2021-1904	https://www. qualcomm.co m/company/ product- security/bull etins/august- 2021-bulletin	H-QUA-SD76- 170921/1369
Loop with Unreachable Exit Condition ('Infinite Loop')	08-Sep-21	5	Loop with unreachable exit condition may occur due to improper handling of unsupported input in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Voice & Music, Snapdragon	https://www. qualcomm.co m/company/ product- security/bull etins/august- 2021-bulletin	H-QUA-SD76- 170921/1370

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Wearables		
			CVE ID : CVE-2021-1914		
Out-of- bounds Write	08-Sep-21	10	Possible buffer underflow due to lack of check for negative indices values when processing user provided input in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Voice & Music, Snapdragon Wearables	https://www. qualcomm.co m/company/ product- security/bull etins/august- 2021-bulletin	H-QUA-SD76- 170921/1371
			CVE ID : CVE-2021-1916		
Integer Underflow (Wrap or Wraparoun d)	08-Sep-21	10	Integer underflow can occur when the RTCP length is lesser than than the actual blocks present in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Voice & Music, Snapdragon Wearables CVE ID : CVE-2021-1919	https://www. qualcomm.co m/company/ product- security/bull etins/august- 2021-bulletin	H-QUA-SD76- 170921/1372
Integer Underflow (Wrap or Wraparoun d)	08-Sep-21	10	Integer underflow can occur due to improper handling of incoming RTCP packets in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Voice & Music, Snapdragon Wearables	https://www. qualcomm.co m/company/ product- security/bull etins/august- 2021-bulletin	H-QUA-SD76- 170921/1373
CVSS Scoring Sc	ale 0-1	1-2	2-3 3-4 4-5 5-6	6-7 7-8	8-9 9-10

Exposure of	Sep-21	4.6	CVE ID : CVE-2021-1920 Incorrect pointer argument passed to trusted application TA could result in un- intended memory operations in Snapdragon Auto, Snapdragon Compute,	https://www. qualcomm.co m/company/ product-	H-QUA-SD76-
Type Conversion or Cast08-SExposure of Resource to Wrong08-S	Sep-21	4.6	passed to trusted application TA could result in un- intended memory operations in Snapdragon Auto, Snapdragon Compute,	qualcomm.co m/company/	H-OUA-SD76-
Resource to Wrong 08-S			Snapdragon Connectivity, Snapdragon Industrial IOT CVE ID : CVE-2021-1923	security/bull etins/august- 2021-bulletin	170921/1374
	Sep-21	2.1	Lack of strict validation of bootmode can lead to information disclosure in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wearables CVE ID : CVE-2021-1929	https://www. qualcomm.co m/company/ product- security/bull etins/august- 2021-bulletin	H-QUA-SD76- 170921/1375
Improper Restriction of Operations within the Bounds of a Memory Buffer	Sep-21	3.6	Possible out of bounds read due to incorrect validation of incoming buffer length in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile CVE ID : CVE-2021-1930	https://www. qualcomm.co m/company/ product- security/bull etins/august- 2021-bulletin	H-QUA-SD76- 170921/1376
Buffer Copy without Checking Size of Input 08-S ('Classic Buffer Overflow')	Sep-21	10	Possible buffer overflow due to improper validation of device types during P2P search in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity,	https://www. qualcomm.co m/company/ product- security/bull etins/august-	H-QUA-SD76- 170921/1377

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking CVE ID : CVE-2021-1972		
sd768g					
Exposure of Resource to Wrong Sphere	08-Sep-21	2.1	Child process can leak information from parent process due to numeric pids are getting compared and these pid can be reused in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wearables	https://www. qualcomm.co m/company/ product- security/bull etins/august- 2021-bulletin	H-QUA-SD76- 170921/1378
Loop with Unreachable Exit Condition ('Infinite Loop')	08-Sep-21	5	CVE ID : CVE-2021-1904 Loop with unreachable exit condition may occur due to improper handling of unsupported input in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Voice & Music, Snapdragon Wearables CVE ID : CVE-2021-1914	https://www. qualcomm.co m/company/ product- security/bull etins/august- 2021-bulletin	H-QUA-SD76- 170921/1379
Out-of- bounds	08-Sep-21	10	Possible buffer underflow due to lack of check for	https://www. qualcomm.co	H-QUA-SD76- 170921/1380

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Write			negative indices values when processing user provided input in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Voice & Music, Snapdragon Wearables CVE ID : CVE-2021-1916	m/company/ product- security/bull etins/august- 2021-bulletin	
Integer Underflow (Wrap or Wraparoun d)	08-Sep-21	10	Integer underflow can occur when the RTCP length is lesser than than the actual blocks present in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Voice & Music, Snapdragon Wearables CVE ID : CVE-2021-1919	https://www. qualcomm.co m/company/ product- security/bull etins/august- 2021-bulletin	H-QUA-SD76- 170921/1381
Integer Underflow (Wrap or Wraparoun d)	08-Sep-21	10	Integer underflow can occur due to improper handling of incoming RTCP packets in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Voice & Music, Snapdragon Wearables	https://www. qualcomm.co m/company/ product- security/bull etins/august- 2021-bulletin	H-QUA-SD76- 170921/1382
Incorrect	08-Sep-21	4.6	CVE ID : CVE-2021-1920 Incorrect pointer argument	https://www.	H-QUA-SD76-
Type Conversion	00-369-21	7.0	passed to trusted application TA could result in un-	qualcomm.co m/company/	170921/1383

CVSS Scoring Scale	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10
			Р	age 488 c	of 1474					

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
or Cast			intended memory operations in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Industrial IOT CVE ID : CVE-2021-1923	product- security/bull etins/august- 2021-bulletin	
Exposure of Resource to Wrong Sphere	08-Sep-21	2.1	Lack of strict validation of bootmode can lead to information disclosure in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wearables CVE ID : CVE-2021-1929	https://www. qualcomm.co m/company/ product- security/bull etins/august- 2021-bulletin	H-QUA-SD76- 170921/1384
Improper Restriction of Operations within the Bounds of a Memory Buffer	08-Sep-21	3.6	Possible out of bounds read due to incorrect validation of incoming buffer length in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile CVE ID : CVE-2021-1930	https://www. qualcomm.co m/company/ product- security/bull etins/august- 2021-bulletin	H-QUA-SD76- 170921/1385
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	08-Sep-21	10	Possible buffer overflow due to improper validation of device types during P2P search in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables,	https://www. qualcomm.co m/company/ product- security/bull etins/august- 2021-bulletin	H-QUA-SD76- 170921/1386

0-1

1-2 2-3 4-5

5-6

6-7

7-8

8-9

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Snapdragon Wired Infrastructure and Networking		
			CVE ID : CVE-2021-1972		
sd778g					
Exposure of Resource to Wrong Sphere	08-Sep-21	2.1	Child process can leak information from parent process due to numeric pids are getting compared and these pid can be reused in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wearables CVE ID : CVE-2021-1904	H-QUA-SD77- 170921/1387	
Loop with Unreachable Exit Condition ('Infinite Loop')	08-Sep-21	5	Loop with unreachable exit condition may occur due to improper handling of unsupported input in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Voice & Music, Snapdragon Wearables CVE ID : CVE-2021-1914	https://www. qualcomm.co m/company/ product- security/bull etins/august- 2021-bulletin	H-QUA-SD77- 170921/1388
Out-of- bounds Write	08-Sep-21	10	Possible buffer underflow due to lack of check for negative indices values when processing user provided input in Snapdragon Auto, Snapdragon Compute,	https://www. qualcomm.co m/company/ product- security/bull etins/august-	H-QUA-SD77- 170921/1389
CVSS Scoring Sc	ale 0-1	1-2	2-3 3-4 4-5 5-6	6-7 7-8	8-9 9-10

Publish Date	CVSS	Description & CVE ID Patc		NCIIPC ID
		Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Voice & Music, Snapdragon Wearables	2021-bulletin	
		CVE ID : CVE-2021-1916		
08-Sep-21	10	Integer underflow can occur when the RTCP length is lesser than than the actual blocks present in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Voice & Music, Snapdragon Wearables	https://www. qualcomm.co m/company/ product- security/bull etins/august- 2021-bulletin	H-QUA-SD77- 170921/1390
		CVE ID : CVE-2021-1919		
08-Sep-21	10	Integer underflow can occur due to improper handling of incoming RTCP packets in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Voice & Music, Snapdragon Wearables CVE ID : CVE-2021-1920	https://www. qualcomm.co m/company/ product- security/bull etins/august- 2021-bulletin	H-QUA-SD77- 170921/1391
08-Sep-21	4.6	Incorrect pointer argument passed to trusted application TA could result in un- intended memory operations in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity,	https://www. qualcomm.co m/company/ product- security/bull etins/august- 2021-bulletin	H-QUA-SD77- 170921/1392
	08-Sep-21	08-Sep-21 10 08-Sep-21 10	08-Sep-21Integer underflow can occur when the RTCP length is lesser than than the actual blocks present in Snapdragon Voice & Music, Snapdragon Wearables08-Sep-211010Integer underflow can occur when the RTCP length is lesser than than the actual blocks present in Snapdragon Voice & Music, Snapdragon Auto, Snapdragon Compute, Snapdragon Industrial IOT, Snapdragon Industrial IOT, Snapdragon Industrial IOT, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Auto, Snapdragon Compute, Snapdragon Industrial IOT, Snapdragon Industrial IOT, Sna	08-Sep-21110Snapdragon Connectivity, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Voice & Music, Snapdragon Wearables2021-bulletin08-Sep-21110Integer underflow can occur when the RTCP length is lesser than than the actual blocks present in Snapdragon Auto, Snapdragon Consumer IOT, Snapdragon Consumer IOT, Snapdragon IoT, Snapdragon Auto, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Voice & Music, Snapdragon Voice & Musi

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Snapdragon Industrial IOT		
			CVE ID : CVE-2021-1923		
Exposure of Resource to Wrong Sphere	08-Sep-21	2.1	Lack of strict validation of bootmode can lead to information disclosure in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wearables CVE ID : CVE-2021-1929	https://www. qualcomm.co m/company/ product- security/bull etins/august- 2021-bulletin	H-QUA-SD77- 170921/1393
Improper Restriction of Operations within the Bounds of a Memory Buffer	08-Sep-21	3.6	Possible out of bounds read due to incorrect validation of incoming buffer length in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile CVE ID : CVE-2021-1930	https://www. qualcomm.co m/company/ product- security/bull etins/august- 2021-bulletin	H-QUA-SD77- 170921/1394
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	08-Sep-21	10	Possible buffer overflow due to improper validation of device types during P2P search in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Woice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking CVE ID : CVE-2021-1972	https://www. qualcomm.co m/company/ product- security/bull etins/august- 2021-bulletin	H-QUA-SD77- 170921/1395
CVSS Scoring Sc	ale 0-1	1-2	2-3 3-4 4-5 5-6	6-7 7-8	8-9 9-10

Page 492 of 1474

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
sd780g		I <u></u>			
Exposure of Resource to Wrong Sphere	08-Sep-21	2.1	Child process can leak information from parent process due to numeric pids are getting compared and these pid can be reused in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wearables CVE ID : CVE-2021-1904	https://www. qualcomm.co m/company/ product- security/bull etins/august- 2021-bulletin	H-QUA-SD78- 170921/1396
Out-of- bounds Write	08-Sep-21	10	Possible buffer underflow due to lack of check for negative indices values when processing user provided input in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Voice & Music, Snapdragon Wearables CVE ID : CVE-2021-1916	https://www. qualcomm.co m/company/ product- security/bull etins/august- 2021-bulletin	H-QUA-SD78- 170921/1397
Incorrect Type Conversion or Cast	08-Sep-21	4.6	Incorrect pointer argument passed to trusted application TA could result in un- intended memory operations in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Industrial IOT CVE ID : CVE-2021-1923	https://www. qualcomm.co m/company/ product- security/bull etins/august- 2021-bulletin	H-QUA-SD78- 170921/1398
Exposure of	08-Sep-21	2.1	Lack of strict validation of	https://www.	H-QUA-SD78-
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 & CVE ID	Patch	NCIIPC ID
Resource to Wrong Sphere			bootmode can lead to information disclosure in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wearables CVE ID : CVE-2021-1929	qualcomm.co m/company/ product- security/bull etins/august- 2021-bulletin	170921/1399
Improper Restriction of Operations within the Bounds of a Memory Buffer	08-Sep-21	3.6	Possible out of bounds read due to incorrect validation of incoming buffer length in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile CVE ID : CVE-2021-1930	https://www. qualcomm.co m/company/ product- security/bull etins/august- 2021-bulletin	H-QUA-SD78- 170921/1400
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	08-Sep-21	10	Possible buffer overflow due to improper validation of device types during P2P search in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Woice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking CVE ID : CVE-2021-1972	https://www. qualcomm.co m/company/ product- security/bull etins/august- 2021-bulletin	H-QUA-SD78- 170921/1401
sd7c				I	I
Improper Restriction	08-Sep-21	3.6	Possible out of bounds read due to incorrect validation of	https://www. qualcomm.co	H-QUA-SD7C- 170921/1402
CVSS Scoring Sc	ale 0-1	1-2	2-3 3-4 4-5 5-6 Page 494 of 1474	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			incoming buffer length in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile CVE ID : CVE-2021-1930	m/company/ product- security/bull etins/august- 2021-bulletin	
sd820					
Loop with Unreachable Exit Condition ('Infinite Loop')	08-Sep-21	5	Loop with unreachable exit condition may occur due to improper handling of unsupported input in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Voice & Music, Snapdragon Wearables CVE ID : CVE-2021-1914	https://www. qualcomm.co m/company/ product- security/bull etins/august- 2021-bulletin	H-QUA-SD82- 170921/1403
Out-of- bounds Write	08-Sep-21	10	Possible buffer underflow due to lack of check for negative indices values when processing user provided input in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Voice & Music, Snapdragon Wearables CVE ID : CVE-2021-1916	https://www. qualcomm.co m/company/ product- security/bull etins/august- 2021-bulletin	H-QUA-SD82- 170921/1404
Integer Underflow (Wrap or	08-Sep-21	10	Integer underflow can occur when the RTCP length is lesser than than the actual	https://www. qualcomm.co m/company/	H-QUA-SD82- 170921/1405

Page 495 of 1474

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Wraparoun d)			blocks present in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Voice & Music, Snapdragon Wearables CVE ID : CVE-2021-1919	product- security/bull etins/august- 2021-bulletin	
Integer Underflow (Wrap or Wraparoun d)	08-Sep-21	10	Integer underflow can occur due to improper handling of incoming RTCP packets in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Voice & Music, Snapdragon Wearables CVE ID : CVE-2021-1920	https://www. qualcomm.co m/company/ product- security/bull etins/august- 2021-bulletin	H-QUA-SD82- 170921/1406
sd821					
Loop with Unreachable Exit Condition ('Infinite Loop')	08-Sep-21	5	Loop with unreachable exit condition may occur due to improper handling of unsupported input in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Voice & Music, Snapdragon Wearables CVE ID : CVE-2021-1914	https://www. qualcomm.co m/company/ product- security/bull etins/august- 2021-bulletin	H-QUA-SD82- 170921/1407
Out-of- bounds Write CVSS Scoring Sc	08-Sep-21 ale 0-1	10	Possible buffer underflow due to lack of check for negative indices values when 2-3 3-4 4-5 5-6	https://www. qualcomm.co m/company/	H-QUA-SD82- 170921/1408 8-9 9-10

Weakness	eakness Publish Date CVSS De		Description & CVE ID	Patch	NCIIPC ID
			processing user providedproduct-input in Snapdragon Auto,security/bullSnapdragon Compute,etins/august-Snapdragon Connectivity,2021-bulletinSnapdragon Consumer IOT,Snapdragon Industrial IOT,Snapdragon Industrial IOT,Snapdragon IoT, SnapdragonVoice & Music, SnapdragonWearablesCVE ID : CVE-2021-1916		
Integer Underflow (Wrap or Wraparoun d)	08-Sep-21	10	Integer underflow can occur when the RTCP length is lesser than than the actual blocks present in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Voice & Music, Snapdragon Wearables CVE ID : CVE-2021-1919	https://www. qualcomm.co m/company/ product- security/bull etins/august- 2021-bulletin	H-QUA-SD82- 170921/1409
Integer Underflow (Wrap or Wraparoun d)	08-Sep-21	10	Integer underflow can occur due to improper handling of incoming RTCP packets in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Voice & Music, Snapdragon Wearables CVE ID : CVE-2021-1920	https://www. qualcomm.co m/company/ product- security/bull etins/august- 2021-bulletin	H-QUA-SD82- 170921/1410
sd835					
Exposure of Resource to Wrong	08-Sep-21	2.1	Child process can leak information from parent process due to numeric pids	https://www. qualcomm.co m/company/	H-QUA-SD83- 170921/1411
CVSS Scoring Sca	ale 0-1	1-2	2-3 3-4 4-5 5-6 Page 497 of 1474	6-7 7-8	8-9 9-10

Page 497 of 1474

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Sphere			are getting compared and these pid can be reused in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables CVE ID : CVE-2021-1904	product- security/bull etins/august- 2021-bulletin	
Loop with Unreachable Exit Condition ('Infinite Loop')	08-Sep-21	5	Loop with unreachable exit condition may occur due to improper handling of unsupported input in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Voice & Music, Snapdragon Wearables CVE ID : CVE-2021-1914	https://www. qualcomm.co m/company/ product- security/bull etins/august- 2021-bulletin	H-QUA-SD83- 170921/1412
Out-of- bounds Write	08-Sep-21	10	Possible buffer underflow due to lack of check for negative indices values when processing user provided input in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Voice & Music, Snapdragon Wearables CVE ID : CVE-2021-1916	https://www. qualcomm.co m/company/ product- security/bull etins/august- 2021-bulletin	H-QUA-SD83- 170921/1413
Integer	08-Sep-21	10	Integer underflow can occur	https://www.	H-QUA-SD83-

Page 498 of 1474

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Underflow (Wrap or Wraparoun d)			when the RTCP length is lesser than than the actual blocks present in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Voice & Music, Snapdragon Wearables CVE ID : CVE-2021-1919	qualcomm.co m/company/ product- security/bull etins/august- 2021-bulletin	170921/1414
Integer Underflow (Wrap or Wraparoun d)	08-Sep-21	10	Integer underflow can occur due to improper handling of incoming RTCP packets in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Voice & Music, Snapdragon Wearables CVE ID : CVE-2021-1920	https://www. qualcomm.co m/company/ product- security/bull etins/august- 2021-bulletin	H-QUA-SD83- 170921/1415
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	08-Sep-21	10	Possible buffer overflow due to improper validation of device types during P2P search in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Woice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking CVE ID : CVE-2021-1972	https://www. qualcomm.co m/company/ product- security/bull etins/august- 2021-bulletin	H-QUA-SD83- 170921/1416

CVSS Scoring Scale	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10
			Pa	age 499 o	of 1474					

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
sd845				L	
Exposure of Resource to Wrong Sphere	08-Sep-21	2.1	Child process can leak information from parent process due to numeric pids are getting compared and these pid can be reused in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wearables CVE ID : CVE-2021-1904	https://www. qualcomm.co m/company/ product- security/bull etins/august- 2021-bulletin	H-QUA-SD84- 170921/1417
Loop with Unreachable Exit Condition ('Infinite Loop')	08-Sep-21	5	Loop with unreachable exit condition may occur due to improper handling of unsupported input in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Voice & Music, Snapdragon Wearables CVE ID : CVE-2021-1914	https://www. qualcomm.co m/company/ product- security/bull etins/august- 2021-bulletin	H-QUA-SD84- 170921/1418
Out-of- 08-Sep-21 10 Write 08-Sep-21 10 CVSS Scoring Scale 0-1 1-2		Possible buffer underflow due to lack of check for negative indices values when processing user provided input in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Voice & Music, Snapdragon	https://www. qualcomm.co m/company/ product- security/bull etins/august- 2021-bulletin	H-QUA-SD84- 170921/1419	

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Wearables		
			CVE ID : CVE-2021-1916		
Integer Underflow (Wrap or Wraparoun d)	08-Sep-21	10	Integer underflow can occur when the RTCP length is lesser than than the actual blocks present in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Voice & Music, Snapdragon Wearables	https://www. qualcomm.co m/company/ product- security/bull etins/august- 2021-bulletin	H-QUA-SD84- 170921/1420
			CVE ID : CVE-2021-1919		
Integer Underflow (Wrap or Wraparoun d)	08-Sep-21	10	Integer underflow can occur due to improper handling of incoming RTCP packets in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Voice & Music, Snapdragon Wearables CVE ID : CVE-2021-1920	https://www. qualcomm.co m/company/ product- security/bull etins/august- 2021-bulletin	H-QUA-SD84- 170921/1421
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	08-Sep-21	10	Possible buffer overflow due to improper validation of device types during P2P search in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Woice & Music, Snapdragon Wearables, Snapdragon Wired	https://www. qualcomm.co m/company/ product- security/bull etins/august- 2021-bulletin	H-QUA-SD84- 170921/1422

0-1

1-2

6-7

5-6

7-8

8-9

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Infrastructure and Networking		
			CVE ID : CVE-2021-1972		
sd850				<u> </u>	
Loop with Unreachable Exit Condition ('Infinite Loop')	08-Sep-21	5	Loop with unreachable exit condition may occur due to improper handling of unsupported input in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Voice & Music, Snapdragon Wearables CVE ID : CVE-2021-1914	https://www. qualcomm.co m/company/ product- security/bull etins/august- 2021-bulletin	H-QUA-SD85- 170921/1423
Out-of- bounds Write	08-Sep-21	10	Possible buffer underflow due to lack of check for negative indices values when processing user provided input in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Voice & Music, Snapdragon Wearables CVE ID : CVE-2021-1916	https://www. qualcomm.co m/company/ product- security/bull etins/august- 2021-bulletin	H-QUA-SD85- 170921/1424
Integer Underflow (Wrap or Wraparoun d)	08-Sep-21	10	Integer underflow can occur when the RTCP length is lesser than than the actual blocks present in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT,	https://www. qualcomm.co m/company/ product- security/bull etins/august- 2021-bulletin	H-QUA-SD85- 170921/1425
CVSS Scoring Scale 0-1 1-2 2-3 3-4 4-5 5-6 6-7 7-8 8-9 9-10					

Page 502 of 1474

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Snapdragon IoT, Snapdragon Voice & Music, Snapdragon Wearables		
			CVE ID : CVE-2021-1919		
Integer Underflow (Wrap or Wraparoun d)	08-Sep-21	10	Integer underflow can occur due to improper handling of incoming RTCP packets in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Voice & Music, Snapdragon Wearables	https://www. qualcomm.co m/company/ product- security/bull etins/august- 2021-bulletin	H-QUA-SD85- 170921/1426
			CVE ID : CVE-2021-1920		
sd855				1	1
Exposure of Resource to Wrong Sphere	08-Sep-21	2.1	Child process can leak information from parent process due to numeric pids are getting compared and these pid can be reused in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables CVE ID : CVE-2021-1904	https://www. qualcomm.co m/company/ product- security/bull etins/august- 2021-bulletin	H-QUA-SD85- 170921/1427
Loop with Unreachable Exit Condition ('Infinite Loop')	08-Sep-21	5	Loop with unreachable exit condition may occur due to improper handling of unsupported input in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity,	https://www. qualcomm.co m/company/ product- security/bull etins/august- 2021-bulletin	H-QUA-SD85- 170921/1428
CVSS Scoring Scale 0-1 1-2 2-3 3-4 4-5 5-6 6-7 7-8 8-9 9-10					

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Voice & Music, Snapdragon Wearables CVE ID : CVE-2021-1914		
Out-of- bounds Write	08-Sep-21	10	Possible buffer underflow due to lack of check for negative indices values when processing user provided input in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Voice & Music, Snapdragon Wearables CVE ID : CVE-2021-1916	https://www. qualcomm.co m/company/ product- security/bull etins/august- 2021-bulletin	H-QUA-SD85- 170921/1429
Integer Underflow (Wrap or Wraparoun d)	08-Sep-21	10	Integer underflow can occur when the RTCP length is lesser than than the actual blocks present in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Voice & Music, Snapdragon Wearables CVE ID : CVE-2021-1919	https://www. qualcomm.co m/company/ product- security/bull etins/august- 2021-bulletin	H-QUA-SD85- 170921/1430
Integer Underflow (Wrap or Wraparoun d)	08-Sep-21	10	Integer underflow can occur due to improper handling of incoming RTCP packets in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT,	https://www. qualcomm.co m/company/ product- security/bull etins/august- 2021-bulletin	H-QUA-SD85- 170921/1431
CVSS Scoring Scale 0-1 1-2 2-3 3-4 4-5 5-6 6-7 7-8 8-9 9-10					

 3-4
 4-5
 5-6

 Page 504 of 1474

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Voice & Music, Snapdragon Wearables		
			CVE ID : CVE-2021-1920		
Incorrect Type Conversion or Cast	08-Sep-21	4.6	Incorrect pointer argument passed to trusted application TA could result in un- intended memory operations in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Industrial IOT CVE ID : CVE-2021-1923	https://www. qualcomm.co m/company/ product- security/bull etins/august- 2021-bulletin	H-QUA-SD85- 170921/1432
Exposure of Resource to Wrong Sphere	08-Sep-21	2.1	Lack of strict validation of bootmode can lead to information disclosure in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wearables CVE ID : CVE-2021-1929	https://www. qualcomm.co m/company/ product- security/bull etins/august- 2021-bulletin	H-QUA-SD85- 170921/1433
Improper Restriction of Operations within the Bounds of a Memory Buffer	08-Sep-21	3.6	Possible out of bounds read due to incorrect validation of incoming buffer length in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile CVE ID : CVE-2021-1930	https://www. qualcomm.co m/company/ product- security/bull etins/august- 2021-bulletin	H-QUA-SD85- 170921/1434
Buffer Copy without Checking	08-Sep-21	10	Possible buffer overflow due to improper validation of device types during P2P	https://www. qualcomm.co m/company/	H-QUA-SD85- 170921/1435
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 & CVE ID	Patch	NCIIPC ID
Size of Input ('Classic Buffer Overflow')			search in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking CVE ID : CVE-2021-1972	product- security/bull etins/august- 2021-bulletin	
sd865_5g					
Exposure of Resource to Wrong Sphere	08-Sep-21	2.1	Child process can leak information from parent process due to numeric pids are getting compared and these pid can be reused in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables CVE ID : CVE-2021-1904	https://www. qualcomm.co m/company/ product- security/bull etins/august- 2021-bulletin	H-QUA-SD86- 170921/1436
Loop with Unreachable Exit Condition ('Infinite Loop')	08-Sep-21	5	Loop with unreachable exit condition may occur due to improper handling of unsupported input in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Voice & Music, Snapdragon	https://www. qualcomm.co m/company/ product- security/bull etins/august- 2021-bulletin	H-QUA-SD86- 170921/1437

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
			Wearables		
			CVE ID : CVE-2021-1914		
Out-of- bounds Write	08-Sep-21	10	Possible buffer underflow due to lack of check for negative indices values when processing user provided input in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Voice & Music, Snapdragon Wearables	https://www. qualcomm.co m/company/ product- security/bull etins/august- 2021-bulletin	H-QUA-SD86- 170921/1438
			CVE ID : CVE-2021-1916		
Integer Underflow (Wrap or Wraparoun d)	08-Sep-21	10	Integer underflow can occur when the RTCP length is lesser than than the actual blocks present in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Voice & Music, Snapdragon Wearables CVE ID : CVE-2021-1919	https://www. qualcomm.co m/company/ product- security/bull etins/august- 2021-bulletin	H-QUA-SD86- 170921/1439
Integer Underflow (Wrap or Wraparoun d)	08-Sep-21	10	Integer underflow can occur due to improper handling of incoming RTCP packets in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Voice & Music, Snapdragon Wearables	https://www. qualcomm.co m/company/ product- security/bull etins/august- 2021-bulletin	H-QUA-SD86- 170921/1440
CVSS Scoring Sca	ale 0-1	1-2	2-3 3-4 4-5 5-6	6-7 7-8	8-9 9-10

	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2021-1920		
Incorrect Type Conversion or Cast	08-Sep-21	4.6	Incorrect pointer argument passed to trusted application TA could result in un- intended memory operations in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Industrial IOT CVE ID : CVE-2021-1923	https://www. qualcomm.co m/company/ product- security/bull etins/august- 2021-bulletin	H-QUA-SD86- 170921/1441
Exposure of Resource to Wrong Sphere	08-Sep-21	2.1	Lack of strict validation of bootmode can lead to information disclosure in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wearables CVE ID : CVE-2021-1929	https://www. qualcomm.co m/company/ product- security/bull etins/august- 2021-bulletin	H-QUA-SD86- 170921/1442
Improper Restriction of Operations within the Bounds of a Memory Buffer	08-Sep-21	3.6	Possible out of bounds read due to incorrect validation of incoming buffer length in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile CVE ID : CVE-2021-1930	https://www. qualcomm.co m/company/ product- security/bull etins/august- 2021-bulletin	H-QUA-SD86- 170921/1443
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	08-Sep-21	10	Possible buffer overflow due to improper validation of device types during P2P search in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT,	https://www. qualcomm.co m/company/ product- security/bull etins/august- 2021-bulletin	H-QUA-SD86- 170921/1444

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking CVE ID : CVE-2021-1972		
sd870					
Exposure of Resource to Wrong Sphere	08-Sep-21	2.1	Child process can leak information from parent process due to numeric pids are getting compared and these pid can be reused in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wearables CVE ID : CVE-2021-1904	https://www. qualcomm.co m/company/ product- security/bull etins/august- 2021-bulletin	H-QUA-SD87- 170921/1445
Loop with Unreachable Exit Condition ('Infinite Loop')	08-Sep-21	5	Loop with unreachable exit condition may occur due to improper handling of unsupported input in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Voice & Music, Snapdragon Wearables CVE ID : CVE-2021-1914	https://www. qualcomm.co m/company/ product- security/bull etins/august- 2021-bulletin	H-QUA-SD87- 170921/1446
Out-of- bounds	08-Sep-21	10	Possible buffer underflow due to lack of check for	https://www. qualcomm.co	H-QUA-SD87- 170921/1447

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Write			negative indices values when processing user provided input in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Voice & Music, Snapdragon Wearables CVE ID : CVE-2021-1916	m/company/ product- security/bull etins/august- 2021-bulletin	
Integer Underflow (Wrap or Wraparoun d)	08-Sep-21	10	Integer underflow can occur when the RTCP length is lesser than than the actual blocks present in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Voice & Music, Snapdragon Wearables CVE ID : CVE-2021-1919	https://www. qualcomm.co m/company/ product- security/bull etins/august- 2021-bulletin	H-QUA-SD87- 170921/1448
Integer Underflow (Wrap or Wraparoun d)	08-Sep-21	10	Integer underflow can occur due to improper handling of incoming RTCP packets in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Voice & Music, Snapdragon Wearables	https://www. qualcomm.co m/company/ product- security/bull etins/august- 2021-bulletin	H-QUA-SD87- 170921/1449
Incorrect			CVE ID : CVE-2021-1920 Incorrect pointer argument	https://www.	H-QUA-SD87-
Type Conversion	08-Sep-21	4.6	passed to trusted application TA could result in un-	qualcomm.co m/company/	170921/1450

CVSS Scoring Scale	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10
Page 510 of 1474										

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
or Cast			intended memory operations in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Industrial IOT CVE ID : CVE-2021-1923	product- security/bull etins/august- 2021-bulletin	
Exposure of Resource to Wrong Sphere	08-Sep-21	2.1	Lack of strict validation of bootmode can lead to information disclosure in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wearables CVE ID : CVE-2021-1929	https://www. qualcomm.co m/company/ product- security/bull etins/august- 2021-bulletin	H-QUA-SD87- 170921/1451
Improper Restriction of Operations within the Bounds of a Memory Buffer	08-Sep-21	3.6	Possible out of bounds read due to incorrect validation of incoming buffer length in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile CVE ID : CVE-2021-1930	https://www. qualcomm.co m/company/ product- security/bull etins/august- 2021-bulletin	H-QUA-SD87- 170921/1452
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	08-Sep-21	10	Possible buffer overflow due to improper validation of device types during P2P search in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables,	https://www. qualcomm.co m/company/ product- security/bull etins/august- 2021-bulletin	H-QUA-SD87- 170921/1453

1-2 2-3

0-1

6-7

5-6

7-8

8-9

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Snapdragon Wired Infrastructure and Networking		
			CVE ID : CVE-2021-1972		
sd888					
Exposure of Resource to Wrong Sphere	08-Sep-21	2.1	Child process can leak information from parent process due to numeric pids are getting compared and these pid can be reused in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wearables CVE ID : CVE-2021-1904	https://www. qualcomm.co m/company/ product- security/bull etins/august- 2021-bulletin	H-QUA-SD88- 170921/1454
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	08-Sep-21	10	Possible buffer overflow due to improper validation of device types during P2P search in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Woice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking CVE ID : CVE-2021-1972	https://www. qualcomm.co m/company/ product- security/bull etins/august- 2021-bulletin	H-QUA-SD88- 170921/1455
sd888_5g					
Exposure of Resource to Wrong	08-Sep-21	2.1	Child process can leak information from parent process due to numeric pids	https://www. qualcomm.co m/company/	H-QUA-SD88- 170921/1456
CVSS Scoring Sc	cale 0-1	1-2	2-3 3-4 4-5 5-6 Page 512 of 1474	6-7 7-8	8-9 <mark>9-10</mark>

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Sphere			are getting compared and these pid can be reused in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables CVE ID : CVE-2021-1904	product- security/bull etins/august- 2021-bulletin	
Loop with Unreachable Exit Condition ('Infinite Loop')	08-Sep-21	5	Loop with unreachable exit condition may occur due to improper handling of unsupported input in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Voice & Music, Snapdragon Wearables CVE ID : CVE-2021-1914	https://www. qualcomm.co m/company/ product- security/bull etins/august- 2021-bulletin	H-QUA-SD88- 170921/1457
Out-of- bounds Write	08-Sep-21	10	Possible buffer underflow due to lack of check for negative indices values when processing user provided input in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Voice & Music, Snapdragon Wearables CVE ID : CVE-2021-1916	https://www. qualcomm.co m/company/ product- security/bull etins/august- 2021-bulletin	H-QUA-SD88- 170921/1458
	08-Sep-21	10	Integer underflow can occur	https://www.	H-QUA-SD88-

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Underflow (Wrap or Wraparoun d)			when the RTCP length is lesser than than the actual blocks present in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Voice & Music, Snapdragon Wearables CVE ID : CVE-2021-1919	qualcomm.co m/company/ product- security/bull etins/august- 2021-bulletin	170921/1459
Integer Underflow (Wrap or Wraparoun d)	08-Sep-21	10	Integer underflow can occur due to improper handling of incoming RTCP packets in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Voice & Music, Snapdragon Wearables CVE ID : CVE-2021-1920	https://www. qualcomm.co m/company/ product- security/bull etins/august- 2021-bulletin	H-QUA-SD88- 170921/1460
Incorrect Type Conversion or Cast	08-Sep-21	4.6	Incorrect pointer argument passed to trusted application TA could result in un- intended memory operations in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Industrial IOT CVE ID : CVE-2021-1923	https://www. qualcomm.co m/company/ product- security/bull etins/august- 2021-bulletin	H-QUA-SD88- 170921/1461
Exposure of Resource to Wrong Sphere	08-Sep-21	2.1	Lack of strict validation of bootmode can lead to information disclosure in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity,	https://www. qualcomm.co m/company/ product- security/bull etins/august-	H-QUA-SD88- 170921/1462

0-1

1-2 2-3

3-4

4-5

5-6

6-7

7-8

8-9

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wearables	2021-bulletin	
			CVE ID : CVE-2021-1929		
Improper Restriction of Operations within the Bounds of a Memory Buffer	08-Sep-21	3.6	Possible out of bounds read due to incorrect validation of incoming buffer length in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile	https://www. qualcomm.co m/company/ product- security/bull etins/august- 2021-bulletin	H-QUA-SD88- 170921/1463
			CVE ID : CVE-2021-1930		
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	08-Sep-21	10	Possible buffer overflow due to improper validation of device types during P2P search in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Woice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking CVE ID : CVE-2021-1972	https://www. qualcomm.co m/company/ product- security/bull etins/august- 2021-bulletin	H-QUA-SD88- 170921/1464
sda429w					
Exposure of Resource to Wrong Sphere	08-Sep-21	2.1	Child process can leak information from parent process due to numeric pids are getting compared and these pid can be reused in Snapdragon Auto, Snapdragon Compute,	https://www. qualcomm.co m/company/ product- security/bull etins/august- 2021-bulletin	H-QUA-SDA4- 170921/1465
CVSS Scoring Sc	ale 0-1	1-2	2-3 3-4 4-5 5-6 Page 515 of 1474	6-7 7-8	8-9 9-10

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables CVE ID : CVE-2021-1904		
Loop with Unreachable Exit Condition ('Infinite Loop')	08-Sep-21	5	Loop with unreachable exit condition may occur due to improper handling of unsupported input in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Voice & Music, Snapdragon Wearables CVE ID : CVE-2021-1914	https://www. qualcomm.co m/company/ product- security/bull etins/august- 2021-bulletin	H-QUA-SDA4- 170921/1466
Out-of- bounds Write	08-Sep-21	10	Possible buffer underflow due to lack of check for negative indices values when processing user provided input in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Voice & Music, Snapdragon Wearables CVE ID : CVE-2021-1916	https://www. qualcomm.co m/company/ product- security/bull etins/august- 2021-bulletin	H-QUA-SDA4- 170921/1467
Out-of- bounds Read	08-Sep-21	3.6	Buffer over read could occur due to incorrect check of buffer size while flashing emmc devices in Snapdragon Connectivity, Snapdragon	https://www. qualcomm.co m/company/ product- security/bull	H-QUA-SDA4- 170921/1468

CVSS Scoring Scale	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10
Daga 516 of 1474										

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking CVE ID : CVE-2021-1928	etins/august- 2021-bulletin	
Exposure of Resource to Wrong Sphere	08-Sep-21	2.1	Lack of strict validation of bootmode can lead to information disclosure in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wearables CVE ID : CVE-2021-1929	https://www. qualcomm.co m/company/ product- security/bull etins/august- 2021-bulletin	H-QUA-SDA4- 170921/1469
sdm429w					
Exposure of Resource to Wrong Sphere	08-Sep-21	2.1	Child process can leak information from parent process due to numeric pids are getting compared and these pid can be reused in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wearables CVE ID : CVE-2021-1904	https://www. qualcomm.co m/company/ product- security/bull etins/august- 2021-bulletin	H-QUA-SDM4- 170921/1470
Loop with Unreachable Exit Condition	08-Sep-21	5	Loop with unreachable exit condition may occur due to improper handling of unsupported input in	https://www. qualcomm.co m/company/ product-	H-QUA-SDM4- 170921/1471
CVSS Scoring Sc	ale 0-1	1-2	2-3 3-4 4-5 5-6	6-7 7-8	8-9 9-10

Page 517 of 1474

('Infinite Loop') Out-of- bounds 08-Sep Write 08-Sep Write 08-Sep ('Classic Buffer Copy without Checking Size of Input 08-Sep ('Classic Buffer Overflow')	h Date	CVSS	Description & CVE ID	Patch	NCIIPC ID		
bounds Write 08-Sep And And And And And And And And And And			Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Voice & Music, Snapdragon Wearables CVE ID : CVE-2021-1914	security/bull etins/august- 2021-bulletin			
without Checking Size of Input 08-Sep ('Classic Buffer	p-21	10	Possible buffer underflow due to lack of check for negative indices values when processing user provided input in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Voice & Music, Snapdragon Wearables CVE ID : CVE-2021-1916	https://www. qualcomm.co m/company/ product- security/bull etins/august- 2021-bulletin	H-QUA-SDM4- 170921/1472		
	p-21	10	Possible buffer overflow due to improper validation of device types during P2P search in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Woice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking	https://www. qualcomm.co m/company/ product- security/bull etins/august- 2021-bulletin	H-QUA-SDM4- 170921/1473		
sdm630			CVE ID : CVE-2021-1972				
SUIIOSU							

Page 518 of 1474

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Exposure of Resource to Wrong Sphere	08-Sep-21	2.1	Child process can leak information from parent process due to numeric pids are getting compared and these pid can be reused in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wearables CVE ID : CVE-2021-1904	https://www. qualcomm.co m/company/ product- security/bull etins/august- 2021-bulletin	H-QUA-SDM6- 170921/1474
Loop with Unreachable Exit Condition ('Infinite Loop')	08-Sep-21	5	Loop with unreachable exit condition may occur due to improper handling of unsupported input in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Voice & Music, Snapdragon Wearables CVE ID : CVE-2021-1914	https://www. qualcomm.co m/company/ product- security/bull etins/august- 2021-bulletin	H-QUA-SDM6- 170921/1475
Out-of- bounds Write	08-Sep-21	10	Possible buffer underflow due to lack of check for negative indices values when processing user provided input in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Voice & Music, Snapdragon Wearables	https://www. qualcomm.co m/company/ product- security/bull etins/august- 2021-bulletin	H-QUA-SDM6- 170921/1476
CVSS Scoring Sc	ale 0-1	1-2	2-3 3-4 4-5 5-6 Page 519 of 1474	6-7 7-8	8-9 9-10

Page 519 of 1474

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2021-1916		
Integer Underflow (Wrap or Wraparoun d)	08-Sep-21	10	Integer underflow can occur when the RTCP length is lesser than than the actual blocks present in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Voice & Music, Snapdragon Wearables CVE ID : CVE-2021-1919	https://www. qualcomm.co m/company/ product- security/bull etins/august- 2021-bulletin	H-QUA-SDM6- 170921/1477
Integer Underflow (Wrap or Wraparoun d)	08-Sep-21	10	Integer underflow can occur due to improper handling of incoming RTCP packets in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Voice & Music, Snapdragon Wearables CVE ID : CVE-2021-1920	https://www. qualcomm.co m/company/ product- security/bull etins/august- 2021-bulletin	H-QUA-SDM6- 170921/1478
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	08-Sep-21	10	Possible buffer overflow due to improper validation of device types during P2P search in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Woice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and	https://www. qualcomm.co m/company/ product- security/bull etins/august- 2021-bulletin	H-QUA-SDM6- 170921/1479

CVSS Scoring Scale	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10
Page 520 of 1474										

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Networking		
			CVE ID : CVE-2021-1972		
sdm830					
Exposure of Resource to Wrong Sphere	08-Sep-21	2.1	Child process can leak information from parent process due to numeric pids are getting compared and these pid can be reused in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables	https://www. qualcomm.co m/company/ product- security/bull etins/august- 2021-bulletin	H-QUA-SDM8- 170921/1480
			CVE ID : CVE-2021-1904		
Incorrect Type Conversion or Cast	08-Sep-21	4.6	Incorrect pointer argument passed to trusted application TA could result in un- intended memory operations in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Industrial IOT CVE ID : CVE-2021-1923	https://www. qualcomm.co m/company/ product- security/bull etins/august- 2021-bulletin	H-QUA-SDM8- 170921/1481
Exposure of Resource to Wrong Sphere	08-Sep-21	2.1	Lack of strict validation of bootmode can lead to information disclosure in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wearables CVE ID : CVE-2021-1929	https://www. qualcomm.co m/company/ product- security/bull etins/august- 2021-bulletin	H-QUA-SDM8- 170921/1482

	CVSS Scoring Scale	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8
-	Page 521 of 1474								

8-9 9-10

Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID					
08-Sep-21	10	Possible buffer overflow due to improper validation of device types during P2P search in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Woice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking CVE ID : CVE-2021-1972	https://www. qualcomm.co m/company/ product- security/bull etins/august- 2021-bulletin	H-QUA-SDM8- 170921/1483					
sdw2500									
08-Sep-21	2.1 Child process can leak information from parent process due to numeric pids are getting compared and these pid can be reused in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wearables CVE ID : CVE-2021-1904		https://www. qualcomm.co m/company/ product- security/bull etins/august- 2021-bulletin	H-QUA- SDW2- 170921/1484					
08-Sep-21	5	Loop with unreachable exit condition may occur due to improper handling of unsupported input in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT,	https://www. qualcomm.co m/company/ product- security/bull etins/august- 2021-bulletin	H-QUA- SDW2- 170921/1485					
	08-Sep-21	08-Sep-21 10 08-Sep-21 2.1	08-Sep-21Possible buffer overflow due to improper validation of device types during P2P search in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Mobile, Snapdragon Mobile, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking CVE ID : CVE-2021-197208-Sep-212.1Child process can leak information from parent process due to numeric pids are getting compared and these pid can be reused in Snapdragon Consumer IOT, Snapdragon Mobile, Snapdragon Mired Infrastructure and Networking08-Sep-212.1Child process can leak information from parent process due to numeric pids are getting compared and these pid can be reused in Snapdragon Consumer IOT, Snapdragon Mobile, Snapdragon Mobile, Sna	08-Sep-21Possible buffer overflow due to improper validation of device types during P2P search in Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Mobile, Snapdragon Mobile, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking CVE ID : CVE-2021-1972https://www. qualcomm.co m/company/ product- security/bull etins/august- 2021-bulletin08-Sep-212.1Child process can leak information from parent process due to numeric pids are getting compared and these pid can be reused in Snapdragon Mobile, Snapdragon Consumer IOT, Snapdragon Connectivity, Snapdragon Compute, Snapdragon Compute, Snapdragon Consumer IOT, Snapdragon Consumer IOT, Snapdragon Mobile, Snapdragon Consumer IOT, Snapdragon Consumer IOT, Snapdragon Mobile, Snapdragon Mobile, Snapdragon Consumer IOT, Snapdragon Mobile, Snapdragon Mobile, Snapdragon Mobile, Snapdragon Mobile, Snapdragon Consumer IOT, Snapdragon Mobile, Snapdragon Consumer IOT, Snapdragon Consumer IOT, Snap					

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Snapdragon IoT, Snapdragon Voice & Music, Snapdragon Wearables		
			CVE ID : CVE-2021-1914		
Out-of- bounds Write	08-Sep-21	10	Possible buffer underflow due to lack of check for negative indices values when processing user provided input in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Voice & Music, Snapdragon Wearables	https://www. qualcomm.co m/company/ product- security/bull etins/august- 2021-bulletin	H-QUA- SDW2- 170921/1486
			CVE ID : CVE-2021-1916		
Integer Underflow (Wrap or Wraparoun d)	08-Sep-21	10	Integer underflow can occur when the RTCP length is lesser than than the actual blocks present in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Voice & Music, Snapdragon Wearables	https://www. qualcomm.co m/company/ product- security/bull etins/august- 2021-bulletin	H-QUA- SDW2- 170921/1487
			CVE ID : CVE-2021-1919		
Integer Underflow (Wrap or Wraparoun d)	08-Sep-21	10	Integer underflow can occur due to improper handling of incoming RTCP packets in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon	https://www. qualcomm.co m/company/ product- security/bull etins/august- 2021-bulletin	H-QUA- SDW2- 170921/1488

1-2

0-1

6-7

5-6

7-8

8-9

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Voice & Music, Snapdragon Wearables CVE ID : CVE-2021-1920		
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	08-Sep-21	10	Possible buffer overflow due to improper validation of device types during P2P search in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Woice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking CVE ID : CVE-2021-1972	https://www. qualcomm.co m/company/ product- security/bull etins/august- 2021-bulletin	H-QUA- SDW2- 170921/1489
sdx12	<u> </u>			<u> </u>	
Exposure of Resource to Wrong Sphere	08-Sep-21	2.1	Child process can leak information from parent process due to numeric pids are getting compared and these pid can be reused in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wearables CVE ID : CVE-2021-1904	https://www. qualcomm.co m/company/ product- security/bull etins/august- 2021-bulletin	H-QUA-SDX1- 170921/1490
Loop with Unreachable Exit Condition ('Infinite	08-Sep-21	5	Loop with unreachable exit condition may occur due to improper handling of unsupported input in Snapdragon Auto,	https://www. qualcomm.co m/company/ product- security/bull	H-QUA-SDX1- 170921/1491
CVSS Scoring Sc	ale 0-1	1-2	2-3 3-4 4-5 5-6	6-7 7-8	8-9 9-10

Page 524 of 1474

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Loop')			Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Voice & Music, Snapdragon Wearables CVE ID : CVE-2021-1914	etins/august- 2021-bulletin	
Out-of- bounds Write	08-Sep-21	10	Possible buffer underflow due to lack of check for negative indices values when processing user provided input in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Voice & Music, Snapdragon Wearables CVE ID : CVE-2021-1916	https://www. qualcomm.co m/company/ product- security/bull etins/august- 2021-bulletin	H-QUA-SDX1- 170921/1492
Integer Underflow (Wrap or Wraparoun d)	08-Sep-21	10	Integer underflow can occur when the RTCP length is lesser than than the actual blocks present in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Voice & Music, Snapdragon Wearables CVE ID : CVE-2021-1919	https://www. qualcomm.co m/company/ product- security/bull etins/august- 2021-bulletin	H-QUA-SDX1- 170921/1493
Integer Underflow (Wrap or Wraparoun d)	08-Sep-21	10	Integer underflow can occur due to improper handling of incoming RTCP packets in Snapdragon Auto, Snapdragon Compute,	https://www. qualcomm.co m/company/ product- security/bull	H-QUA-SDX1- 170921/1494

Page 525 of 1474

Size of Input ('Classic 08-Sep-21 10 Shapuragon Mutustrian IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired security/bull etins/august- 2021-bulletin 170921/149 Overflow') Napdragon Wearables, Snapdragon Wired 2021-bulletin 140 Infrastructure and Networking Networking 2021-bulletin 140 sdx20 CVE ID : CVE-2021-1972 149	Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Image: constraint of the constra				Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Voice & Music, Snapdragon	, .	
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')08-Sep-2110to improper validation of device types during P2P search in Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wired Infrastructure and Networkinghttps://www. qualcomm.co m/company/ product- security/bull etins/august- 2021-bulletinH-QUA-SDX1 170921/149sdx205Child process can leak information from parentChild process can leak information from parentI				CVE ID : CVE-2021-1920		
Child process can leak information from parent	without Checking Size of Input ('Classic Buffer	08-Sep-21	10	to improper validation of device types during P2P search in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Woice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking	qualcomm.co m/company/ product- security/bull etins/august-	H-QUA-SDX1- 170921/1495
information from parent	sdx20					
Exposure of Resource to08-Sep-212.1are getting compared and these pid can be reused in Snapdragon Auto, Snapdragon Compute,https://www. qualcomm.co m/company/ product-	Resource to Wrong	08-Sep-21	2.1	information from parent process due to numeric pids are getting compared and these pid can be reused in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wearables	qualcomm.co m/company/ product- security/bull etins/august-	H-QUA-SDX2- 170921/1496
Loop with 08-Sep-21 5 Loop with unreachable exit https://www. H-QUA-SDX2	Loop with	08-Sep-21	5	Loop with unreachable exit	https://www.	H-QUA-SDX2-

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Unreachable Exit Condition ('Infinite Loop')			condition may occur due to improper handling of unsupported input in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Voice & Music, Snapdragon Wearables CVE ID : CVE-2021-1914	qualcomm.co m/company/ product- security/bull etins/august- 2021-bulletin	170921/1497
Out-of- bounds Write	08-Sep-21	10	Possible buffer underflow due to lack of check for negative indices values when processing user provided input in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Voice & Music, Snapdragon Wearables CVE ID : CVE-2021-1916	https://www. qualcomm.co m/company/ product- security/bull etins/august- 2021-bulletin	H-QUA-SDX2- 170921/1498
Integer Underflow (Wrap or Wraparoun d)	08-Sep-21	10	Integer underflow can occur when the RTCP length is lesser than than the actual blocks present in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Voice & Music, Snapdragon Wearables	https://www. qualcomm.co m/company/ product- security/bull etins/august- 2021-bulletin	H-QUA-SDX2- 170921/1499
	08-Sep-21	10	CVE ID : CVE-2021-1919	https://www.	
Integer	00-00-21	10	Integer underflow can occur	https://www.	H-QUA-SDX2-

(Wrap or Wraparoun d)(Wrap or Wraparoun d)(Mraparoun Sinapdragon Compute, Sinapdragon Consumer 10T, Sinapdragon Consumer 10T, Sinapdragon Consumer 10T, Sinapdragon Consumer 10T, Sinapdragon Industrial 10T, Sinapdragon Consumer 10T, Sinapdragon Weidel Sinapdragon Weidel Sinapdra	Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')08-Sep-21Image: Comparison of the comparison o	(Wrap or Wraparoun			incoming RTCP packets in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Voice & Music, Snapdragon Wearables	m/company/ product- security/bull etins/august-	170921/1500
Exposure of Resource to Wrong Sphere08-Sep-212.1Child process can leak information from parent process due to numeric pids these pid can be reused in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile,https://www. qualcomm.co m/company/ product- security/bull etins/august- 2021-bulletinH-QUA-SDX2- 170921/1502	without Checking Size of Input ('Classic Buffer	08-Sep-21	10	to improper validation of device types during P2P search in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Woice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking	qualcomm.co m/company/ product- security/bull etins/august-	H-QUA-SDX2- 170921/1501
Exposure of Resource to Wrong Sphere08-Sep-212.1information from parent process due to numeric pids are getting compared and these pid can be reused in Snapdragon Auto, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile,https://www. qualcomm.co m/company/ product- security/bull etins/august- 2021-bulletinH-QUA-SDX2- H-QUA-SDX2- product- security/bull etins/august- 2021-bulletin	sdx20m					
	Resource to Wrong	08-Sep-21	2.1	information from parent process due to numeric pids are getting compared and these pid can be reused in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile,	qualcomm.co m/company/ product- security/bull etins/august-	H-QUA-SDX2- 170921/1502

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Snapdragon Wearables		
			CVE ID : CVE-2021-1904		
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	08-Sep-21	10	Possible buffer overflow due to improper validation of device types during P2P search in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Woice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking CVE ID : CVE-2021-1972	https://www. qualcomm.co m/company/ product- security/bull etins/august- 2021-bulletin	H-QUA-SDX2- 170921/1503
sdx24					
Exposure of Resource to Wrong Sphere	08-Sep-21	2.1	Child process can leak information from parent process due to numeric pids are getting compared and these pid can be reused in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wearables CVE ID : CVE-2021-1904	https://www. qualcomm.co m/company/ product- security/bull etins/august- 2021-bulletin	H-QUA-SDX2- 170921/1504
Loop with Unreachable Exit Condition ('Infinite Loop')	08-Sep-21	5	Loop with unreachable exit condition may occur due to improper handling of unsupported input in Snapdragon Auto, Snapdragon Compute,	https://www. qualcomm.co m/company/ product- security/bull etins/august-	H-QUA-SDX2- 170921/1505
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 & CVE ID	Patch	NCIIPC ID
			Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Voice & Music, Snapdragon Wearables	2021-bulletin	
			CVE ID : CVE-2021-1914		
Out-of- bounds Write	08-Sep-21	10	Possible buffer underflow due to lack of check for negative indices values when processing user provided input in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Voice & Music, Snapdragon Wearables CVE ID : CVE-2021-1916	https://www. qualcomm.co m/company/ product- security/bull etins/august- 2021-bulletin	H-QUA-SDX2- 170921/1506
Integer Underflow (Wrap or Wraparoun d)	08-Sep-21	10	Integer underflow can occur when the RTCP length is lesser than than the actual blocks present in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Voice & Music, Snapdragon Wearables CVE ID : CVE-2021-1919	https://www. qualcomm.co m/company/ product- security/bull etins/august- 2021-bulletin	H-QUA-SDX2- 170921/1507
Integer Underflow (Wrap or Wraparoun d)	08-Sep-21	10	Integer underflow can occur due to improper handling of incoming RTCP packets in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity,	https://www. qualcomm.co m/company/ product- security/bull etins/august-	H-QUA-SDX2- 170921/1508

0-1

1-2

7-8

5-6

6-7

8-9

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Voice & Music, Snapdragon Wearables CVE ID : CVE-2021-1920	2021-bulletin	
Incorrect Type Conversion or Cast	08-Sep-21	4.6	Incorrect pointer argument passed to trusted application TA could result in un- intended memory operations in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Industrial IOT CVE ID : CVE-2021-1923	https://www. qualcomm.co m/company/ product- security/bull etins/august- 2021-bulletin	H-QUA-SDX2- 170921/1509
Improper Restriction of Operations within the Bounds of a Memory Buffer	08-Sep-21	3.6	Possible out of bounds read due to incorrect validation of incoming buffer length in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile CVE ID : CVE-2021-1930	https://www. qualcomm.co m/company/ product- security/bull etins/august- 2021-bulletin	H-QUA-SDX2- 170921/1510
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	08-Sep-21	10	Possible buffer overflow due to improper validation of device types during P2P search in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Woice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and	https://www. qualcomm.co m/company/ product- security/bull etins/august- 2021-bulletin	H-QUA-SDX2- 170921/1511

0-1

1-2

6-7

5-6

7-8

8-9

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Networking		
			CVE ID : CVE-2021-1972		
sdx50m					
Exposure of Resource to Wrong Sphere	08-Sep-21	2.1	Child process can leak information from parent process due to numeric pids are getting compared and these pid can be reused in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wearables CVE ID : CVE-2021-1904	https://www. qualcomm.co m/company/ product- security/bull etins/august- 2021-bulletin	H-QUA-SDX5- 170921/1512
Loop with Unreachable Exit Condition ('Infinite Loop')	08-Sep-21	5	Loop with unreachable exit condition may occur due to improper handling of unsupported input in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Voice & Music, Snapdragon Wearables CVE ID : CVE-2021-1914	https://www. qualcomm.co m/company/ product- security/bull etins/august- 2021-bulletin	H-QUA-SDX5- 170921/1513
Out-of- bounds Write	08-Sep-21	10	Possible buffer underflow due to lack of check for negative indices values when processing user provided input in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT,	https://www. qualcomm.co m/company/ product- security/bull etins/august- 2021-bulletin	H-QUA-SDX5- 170921/1514
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 Industrial IOT, Snapdragon IoT, Snapdragon Voice & Music, Snapdragon Wearables		
			CVE ID : CVE-2021-1916		
Integer Underflow (Wrap or Wraparoun d)	08-Sep-21	10	Integer underflow can occur when the RTCP length is lesser than than the actual blocks present in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Voice & Music, Snapdragon Wearables CVE ID : CVE-2021-1919	https://www. qualcomm.co m/company/ product- security/bull etins/august- 2021-bulletin	H-QUA-SDX5- 170921/1515
Integer Underflow (Wrap or Wraparoun d)	08-Sep-21	10	Integer underflow can occur due to improper handling of incoming RTCP packets in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Voice & Music, Snapdragon Wearables CVE ID : CVE-2021-1920	https://www. qualcomm.co m/company/ product- security/bull etins/august- 2021-bulletin	H-QUA-SDX5- 170921/1516
Incorrect Type Conversion or Cast	08-Sep-21	4.6	Incorrect pointer argument passed to trusted application TA could result in un- intended memory operations in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Industrial IOT CVE ID : CVE-2021-1923	https://www. qualcomm.co m/company/ product- security/bull etins/august- 2021-bulletin	H-QUA-SDX5- 170921/1517
CVSS Scoring Sc	ale 0-1	1-2	2-3 3-4 4-5 5-6 Page 533 of 1474	6-7 7-8	8-9 9-10

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Exposure of Resource to Wrong Sphere	08-Sep-21	2.1	Lack of strict validation of bootmode can lead to information disclosure in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wearables CVE ID : CVE-2021-1929	https://www. qualcomm.co m/company/ product- security/bull etins/august- 2021-bulletin	H-QUA-SDX5- 170921/1518
Improper Restriction of Operations within the Bounds of a Memory Buffer	08-Sep-21	3.6	Possible out of bounds read due to incorrect validation of incoming buffer length in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile CVE ID : CVE-2021-1930	https://www. qualcomm.co m/company/ product- security/bull etins/august- 2021-bulletin	H-QUA-SDX5- 170921/1519
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	08-Sep-21	10	Possible buffer overflow due to improper validation of device types during P2P search in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Woice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking CVE ID : CVE-2021-1972	https://www. qualcomm.co m/company/ product- security/bull etins/august- 2021-bulletin	H-QUA-SDX5- 170921/1520
sdx55					
Exposure of	08-Sep-21	2.1	Child process can leak	https://www.	H-QUA-SDX5-
CVSS Scoring Sc	ale 0-1	1-2	2-3 3-4 4-5 5-6 Page 534 of 1474	6-7 7-8	8-9 9-10

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Resource to Wrong Sphere			information from parent process due to numeric pids are getting compared and these pid can be reused in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wearables CVE ID : CVE-2021-1904	qualcomm.co m/company/ product- security/bull etins/august- 2021-bulletin	170921/1521
Loop with Unreachable Exit Condition ('Infinite Loop')	08-Sep-21	5	Loop with unreachable exit condition may occur due to improper handling of unsupported input in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Voice & Music, Snapdragon Wearables CVE ID : CVE-2021-1914	https://www. qualcomm.co m/company/ product- security/bull etins/august- 2021-bulletin	H-QUA-SDX5- 170921/1522
Out-of- bounds Write	08-Sep-21	10	Possible buffer underflow due to lack of check for negative indices values when processing user provided input in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Voice & Music, Snapdragon Wearables	https://www. qualcomm.co m/company/ product- security/bull etins/august- 2021-bulletin	H-QUA-SDX5- 170921/1523

CVSS Scoring Scale	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10
Page 535 of 1474										

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2021-1916		
Integer Underflow (Wrap or Wraparoun d)	08-Sep-21	10	Integer underflow can occur when the RTCP length is lesser than than the actual blocks present in Snapdragon Auto, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Voice & Music, Snapdragon Wearableshttps:// qualcom m/comp product 		H-QUA-SDX5- 170921/1524
Integer Underflow (Wrap or Wraparoun d)	08-Sep-21	10	Integer underflow can occur due to improper handling of incoming RTCP packets in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Voice & Music, Snapdragon Wearables CVE ID : CVE-2021-1920	https://www. qualcomm.co m/company/ product- security/bull etins/august- 2021-bulletin	H-QUA-SDX5- 170921/1525
Incorrect Type Conversion or Cast	08-Sep-21	4.6	Incorrect pointer argument passed to trusted application TA could result in un- intended memory operations in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Industrial IOT CVE ID : CVE-2021-1923	https://www. qualcomm.co m/company/ product- security/bull etins/august- 2021-bulletin	H-QUA-SDX5- 170921/1526
Exposure of Resource to Wrong Sphere CVSS Scoring Sc	08-Sep-21 ale 0-1	2.1	Lack of strict validation of bootmode can lead to information disclosure in Snapdragon Auto, 2-3 3-4 4-5 5-6	https://www. qualcomm.co m/company/ product-	H-QUA-SDX5- 170921/1527 8-9 9-10

Page 536 of 1474

Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
		Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wearables	security/bull etins/august- 2021-bulletin	
		CVE ID : CVE-2021-1929		
08-Sep-21	3.6	Possible out of bounds read due to incorrect validation of incoming buffer length in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile	https://www. qualcomm.co m/company/ product- security/bull etins/august- 2021-bulletin	H-QUA-SDX5- 170921/1528
08-Sep-21	10	to improper validation of device types during P2P search in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Woice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking CVE ID : CVE-2021-1972	https://www. qualcomm.co m/company/ product- security/bull etins/august- 2021-bulletin	H-QUA-SDX5- 170921/1529
		Child process can loak	https://www.	
08-Sep-21	2.1	information from parent process due to numeric pids are getting compared and these pid can be reused in	qualcomm.co m/company/ product- security/bull	H-QUA-SDX5- 170921/1530
	08-Sep-21	08-Sep-21 3.6 08-Sep-21 10	Image: construct of the state of the stat	08-Sep-211Snapdragon Compute, Snapdragon Connectivity, Snapdragon Mobile, Snapdragon Mobile, Snapdragon Wearablessecurity/bull etins/august- 2021-bulletin08-Sep-2113.6Possible out of bounds read due to incorrect validation of incoming buffer length in Snapdragon Consumer IOT, Snapdragon Consumer IOT, Snapdragon Compute, Snapdragon Consumer IOT, Snapdragon Micte Snapdragon Micte Snapdragon Wearables, Snapdragon Wired Infrastructure and Networkinghttps://www. security/bull etins/august- 2021-bulletin08-Sep-2112.1Child process can leak information from parent process due to numeric pids are getting compared andhttps://www. qualcom.co m/company/ product-

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables CVE ID : CVE-2021-1904	etins/august- 2021-bulletin	
Loop with Unreachable Exit Condition ('Infinite Loop')	08-Sep-21	5	Loop with unreachable exit condition may occur due to improper handling of unsupported input in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Voice & Music, Snapdragon Wearables CVE ID : CVE-2021-1914	https://www. qualcomm.co m/company/ product- security/bull etins/august- 2021-bulletin	H-QUA-SDX5- 170921/1531
Out-of- bounds Write	08-Sep-21	10	Possible buffer underflow due to lack of check for negative indices values when processing user provided input in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Voice & Music, Snapdragon Wearables CVE ID : CVE-2021-1916	https://www. qualcomm.co m/company/ product- security/bull etins/august- 2021-bulletin	H-QUA-SDX5- 170921/1532
Integer Underflow (Wrap or	08-Sep-21	10	Integer underflow can occur when the RTCP length is lesser than than the actual	https://www. qualcomm.co m/company/	H-QUA-SDX5- 170921/1533

CVSS Scoring Scale	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10
Page 538 of 1474										

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Wraparoun d)			blocks present in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Voice & Music, Snapdragon Wearables CVE ID : CVE-2021-1919	product- security/bull etins/august- 2021-bulletin	
Integer Underflow (Wrap or Wraparoun d)	08-Sep-21	10	Integer underflow can occur due to improper handling of incoming RTCP packets in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Voice & Music, Snapdragon Wearables CVE ID : CVE-2021-1920	https://www. qualcomm.co m/company/ product- security/bull etins/august- 2021-bulletin	H-QUA-SDX5- 170921/1534
Incorrect Type Conversion or Cast	08-Sep-21	4.6	Incorrect pointer argument passed to trusted application TA could result in un- intended memory operations in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Industrial IOT CVE ID : CVE-2021-1923	https://www. qualcomm.co m/company/ product- security/bull etins/august- 2021-bulletin	H-QUA-SDX5- 170921/1535
Exposure of Resource to Wrong Sphere	08-Sep-21	2.1	Lack of strict validation of bootmode can lead to information disclosure in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT,	https://www. qualcomm.co m/company/ product- security/bull etins/august- 2021-bulletin	H-QUA-SDX5- 170921/1536

0-1

1-2

5-6

6-7

7-8

8-9

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID	
			Snapdragon Mobile, Snapdragon Wearables CVE ID : CVE-2021-1929			
Improper Restriction of Operations within the Bounds of a Memory Buffer	08-Sep-21	3.6	Possible out of bounds read due to incorrect validation of incoming buffer length in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile CVE ID : CVE-2021-1930	https://www. qualcomm.co m/company/ product- security/bull etins/august- 2021-bulletin	H-QUA-SDX5- 170921/1537	
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	08-Sep-21	10	Possible buffer overflow due to improper validation of device types during P2P search in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Woice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking CVE ID : CVE-2021-1972	https://www. qualcomm.co m/company/ product- security/bull etins/august- 2021-bulletin	H-QUA-SDX5- 170921/1538	
sdxr1						
Exposure of Resource to Wrong Sphere	08-Sep-21	2.1	Child process can leak information from parent process due to numeric pids are getting compared and these pid can be reused in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT,	https://www. qualcomm.co m/company/ product- security/bull etins/august- 2021-bulletin	H-QUA-SDXR- 170921/1539	
CVSS Scoring Scale 0-1 1-2 2-3 3-4 4-5 5-6 6-7 7-8 8-9 9-10						

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables		
			CVE ID : CVE-2021-1904		
Loop with Unreachable Exit Condition ('Infinite Loop')	08-Sep-21	5	Loop with unreachable exit condition may occur due to improper handling of unsupported input in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Voice & Music, Snapdragon Wearables	https://www. qualcomm.co m/company/ product- security/bull etins/august- 2021-bulletin	H-QUA-SDXR- 170921/1540
			CVE ID : CVE-2021-1914		
Out-of- bounds Write	08-Sep-21	10	Possible buffer underflow due to lack of check for negative indices values when processing user provided input in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Voice & Music, Snapdragon Wearables CVE ID : CVE-2021-1916	https://www. qualcomm.co m/company/ product- security/bull etins/august- 2021-bulletin	H-QUA-SDXR- 170921/1541
Integer Underflow (Wrap or Wraparoun d)	08-Sep-21	10	Integer underflow can occur when the RTCP length is lesser than than the actual blocks present in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT,	https://www. qualcomm.co m/company/ product- security/bull etins/august- 2021-bulletin	H-QUA-SDXR- 170921/1542
CVSS Scoring Sc	ale 0-1	1-2	2-3 3-4 4-5 5-6	6-7 7-8	8-9 9-10

 3-4
 4-5
 5-6
 6-7

 Page 541 of 1474

Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
		Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Voice & Music, Snapdragon Wearables		
		CVE ID : CVE-2021-1919		
08-Sep-21	10	Integer underflow can occur due to improper handling of incoming RTCP packets in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Voice & Music, Snapdragon Wearables CVE ID : CVE-2021-1920	https://www. qualcomm.co m/company/ product- security/bull etins/august- 2021-bulletin	H-QUA-SDXR- 170921/1543
08-Sep-21	10	Possible buffer overflow due to improper validation of device types during P2P search in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Industrial IOT, Snapdragon Woile, Snapdragon Woice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking CVE ID : CVE-2021-1972	https://www. qualcomm.co m/company/ product- security/bull etins/august- 2021-bulletin	H-QUA-SDXR- 170921/1544
08-Sep-21	2.1	Child process can leak information from parent process due to numeric pids are getting compared and these pid can be reused in	https://www. qualcomm.co m/company/ product- security/bull	H-QUA-SDXR- 170921/1545
	08-Sep-21	08-Sep-21 10 08-Sep-21 10	Image: construct of the second seco	08-Sep-21110Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Voice & Music, Snapdragon WearablesHttps://www. qualcomm.co m/company/ product- security/bull etins/august- 2021-bulletin08-Sep-21110Napdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Iot, Snapdragon Snapdragon Consumer IOT, Snapdragon Iot, Snapdragon Voice & Music, Snapdragon Iot, Snapdragon Voice & Music, Snapdragon Voice & Music, Snapdragon Voice & Music, Snapdragon Iot, Snapdragon Voice & Music, Snapdragon Voice & Music, Snapdragon Voice & Music, Snapdragon Iot, Snapdragon Voice & Music, Snapdragon Auto, Snapdragon Consumer IOT, Snapdragon Consumer IOT, Snapdragon Consumer IOT, Snapdragon Noile, Snapdragon Nice & Music, Snapdragon Nice & Music, Snapdragon Wired Infrastructure and Networkinghttps://www. qualcomm.co m/company/ product- security/bull etins/august- 2021-bulletin08-Sep-2112.11Child process can leak information from parent process due to numeric pids are getting compared andhttps://www. qualcomm.co m/company/ product-

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables CVE ID : CVE-2021-1904	etins/august- 2021-bulletin	
Loop with Unreachable Exit Condition ('Infinite Loop')	08-Sep-21	5	Loop with unreachable exit condition may occur due to improper handling of unsupported input in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Voice & Music, Snapdragon Wearables CVE ID : CVE-2021-1914	https://www. qualcomm.co m/company/ product- security/bull etins/august- 2021-bulletin	H-QUA-SDXR- 170921/1546
Out-of- bounds Write	08-Sep-21	10	Possible buffer underflow due to lack of check for negative indices values when processing user provided input in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Voice & Music, Snapdragon Wearables CVE ID : CVE-2021-1916	https://www. qualcomm.co m/company/ product- security/bull etins/august- 2021-bulletin	H-QUA-SDXR- 170921/1547
Integer Underflow (Wrap or	08-Sep-21	10	Integer underflow can occur when the RTCP length is lesser than than the actual	https://www. qualcomm.co m/company/	H-QUA-SDXR- 170921/1548

CVSS Scoring Scale	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10
Page 5/2 of 1/7/										

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Wraparoun d)			blocks present in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Voice & Music, Snapdragon Wearables CVE ID : CVE-2021-1919	product- security/bull etins/august- 2021-bulletin	
Integer Underflow (Wrap or Wraparoun d)	08-Sep-21	10	Integer underflow can occur due to improper handling of incoming RTCP packets in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Voice & Music, Snapdragon Wearables CVE ID : CVE-2021-1920	https://www. qualcomm.co m/company/ product- security/bull etins/august- 2021-bulletin	H-QUA-SDXR- 170921/1549
Incorrect Type Conversion or Cast	08-Sep-21	4.6	Incorrect pointer argument passed to trusted application TA could result in un- intended memory operations in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Industrial IOT CVE ID : CVE-2021-1923	https://www. qualcomm.co m/company/ product- security/bull etins/august- 2021-bulletin	H-QUA-SDXR- 170921/1550
Exposure of Resource to Wrong Sphere	08-Sep-21	2.1	Lack of strict validation of bootmode can lead to information disclosure in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT,	https://www. qualcomm.co m/company/ product- security/bull etins/august- 2021-bulletin	H-QUA-SDXR- 170921/1551

0-1

1-2

5-6

6-7

7-8

8-9

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Snapdragon Mobile, Snapdragon Wearables CVE ID : CVE-2021-1929		
Improper Restriction of Operations within the Bounds of a Memory Buffer	08-Sep-21	3.6	Possible out of bounds read due to incorrect validation of incoming buffer length in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile CVE ID : CVE-2021-1930	https://www. qualcomm.co m/company/ product- security/bull etins/august- 2021-bulletin	H-QUA-SDXR- 170921/1552
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	08-Sep-21	10	Possible buffer overflow due to improper validation of device types during P2P search in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Woice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking CVE ID : CVE-2021-1972	https://www. qualcomm.co m/company/ product- security/bull etins/august- 2021-bulletin	H-QUA-SDXR- 170921/1553
sd_455					
Exposure of Resource to Wrong Sphere	08-Sep-21	2.1	Child process can leak information from parent process due to numeric pids are getting compared and these pid can be reused in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT,	https://www. qualcomm.co m/company/ product- security/bull etins/august- 2021-bulletin	H-QUA-SD_4- 170921/1554
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 & CVE ID	Patch	NCIIPC ID
			Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables		
			CVE ID : CVE-2021-1904		
Loop with Unreachable Exit Condition ('Infinite Loop')	08-Sep-21	5	Loop with unreachable exit condition may occur due to improper handling of unsupported input in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Voice & Music, Snapdragon Wearables	https://www. qualcomm.co m/company/ product- security/bull etins/august- 2021-bulletin	H-QUA-SD_4- 170921/1555
			CVE ID : CVE-2021-1914		
Out-of- bounds Write	08-Sep-21	10	Possible buffer underflow due to lack of check for negative indices values when processing user provided input in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Voice & Music, Snapdragon Wearables CVE ID : CVE-2021-1916	https://www. qualcomm.co m/company/ product- security/bull etins/august- 2021-bulletin	H-QUA-SD_4- 170921/1556
Integer Underflow (Wrap or Wraparoun d)	08-Sep-21	10	Integer underflow can occur when the RTCP length is lesser than than the actual blocks present in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT,	https://www. qualcomm.co m/company/ product- security/bull etins/august- 2021-bulletin	H-QUA-SD_4- 170921/1557
CVSS Scoring Sc	ale 0-1	1-2	2-3 3-4 4-5 5-6	6-7 7-8	8-9 9-10

 3-4
 4-5
 5-6
 6-7

 Page 546 of 1474

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Voice & Music, Snapdragon Wearables		
			CVE ID : CVE-2021-1919		
Integer Underflow (Wrap or Wraparoun d)	08-Sep-21	10	Integer underflow can occur due to improper handling of incoming RTCP packets in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Voice & Music, Snapdragon Wearables CVE ID : CVE-2021-1920	https://www. qualcomm.co m/company/ product- security/bull etins/august- 2021-bulletin	H-QUA-SD_4- 170921/1558
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	08-Sep-21	10	Possible buffer overflow due to improper validation of device types during P2P search in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Woice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking CVE ID : CVE-2021-1972	https://www. qualcomm.co m/company/ product- security/bull etins/august- 2021-bulletin	H-QUA-SD_4- 170921/1559
sd_636					
Exposure of Resource to Wrong Sphere	08-Sep-21	2.1	Child process can leak information from parent process due to numeric pids are getting compared and these pid can be reused in	https://www. qualcomm.co m/company/ product- security/bull	H-QUA-SD_6- 170921/1560

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables CVE ID : CVE-2021-1904	etins/august- 2021-bulletin	
Loop with Unreachable Exit Condition ('Infinite Loop')	08-Sep-21	5	Loop with unreachable exit condition may occur due to improper handling of unsupported input in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Voice & Music, Snapdragon Wearables CVE ID : CVE-2021-1914	https://www. qualcomm.co m/company/ product- security/bull etins/august- 2021-bulletin	H-QUA-SD_6- 170921/1561
Out-of- bounds Write	08-Sep-21	10	Possible buffer underflow due to lack of check for negative indices values when processing user provided input in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Voice & Music, Snapdragon Wearables CVE ID : CVE-2021-1916	https://www. qualcomm.co m/company/ product- security/bull etins/august- 2021-bulletin	H-QUA-SD_6- 170921/1562
Integer Underflow (Wrap or	08-Sep-21	10	Integer underflow can occur when the RTCP length is lesser than than the actual	https://www. qualcomm.co m/company/	H-QUA-SD_6- 170921/1563

CVSS Scoring Scale	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10
Page 548 of 1474										

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Wraparoun d)			blocks present in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Voice & Music, Snapdragon Wearables	product- security/bull etins/august- 2021-bulletin	
			CVE ID : CVE-2021-1919		
Integer Underflow (Wrap or Wraparoun d)	08-Sep-21	10	Integer underflow can occur due to improper handling of incoming RTCP packets in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Voice & Music, Snapdragon Wearables CVE ID : CVE-2021-1920	https://www. qualcomm.co m/company/ product- security/bull etins/august- 2021-bulletin	H-QUA-SD_6- 170921/1564
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	08-Sep-21	10	Possible buffer overflow due to improper validation of device types during P2P search in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Industrial IOT, Snapdragon Woile, Snapdragon Woice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking CVE ID : CVE-2021-1972	https://www. qualcomm.co m/company/ product- security/bull etins/august- 2021-bulletin	H-QUA-SD_6- 170921/1565
sd_675				·	·
Exposure of	08-Sep-21	2.1	Child process can leak	https://www.	H-QUA-SD_6-
CVSS Scoring Sc	cale 0-1	1-2	2-3 3-4 4-5 5-6 Page 549 of 1474	6-7 7-8	8-9 9-10

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Resource to Wrong Sphere			information from parent process due to numeric pids are getting compared and these pid can be reused in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wearables CVE ID : CVE-2021-1904	qualcomm.co m/company/ product- security/bull etins/august- 2021-bulletin	170921/1566
Loop with Unreachable Exit Condition ('Infinite Loop')	08-Sep-21	5	Loop with unreachable exit condition may occur due to improper handling of unsupported input in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Voice & Music, Snapdragon Wearables CVE ID : CVE-2021-1914	https://www. qualcomm.co m/company/ product- security/bull etins/august- 2021-bulletin	H-QUA-SD_6- 170921/1567
Out-of- bounds Write	08-Sep-21	10	Possible buffer underflow due to lack of check for negative indices values when processing user provided input in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Voice & Music, Snapdragon Wearables	https://www. qualcomm.co m/company/ product- security/bull etins/august- 2021-bulletin	H-QUA-SD_6- 170921/1568

CVSS Scoring Scale	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10
Page 550 of 1474										

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2021-1916		
Integer Underflow (Wrap or Wraparoun d)	08-Sep-21	10	Integer underflow can occur when the RTCP length is lesser than than the actual blocks present in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Voice & Music, Snapdragon Wearables CVE ID : CVE-2021-1919	https://www. qualcomm.co m/company/ product- security/bull etins/august- 2021-bulletin	H-QUA-SD_6- 170921/1569
Integer Underflow (Wrap or Wraparoun d)	08-Sep-21	10	Integer underflow can occur due to improper handling of incoming RTCP packets in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Voice & Music, Snapdragon Wearables CVE ID : CVE-2021-1920	https://www. qualcomm.co m/company/ product- security/bull etins/august- 2021-bulletin	H-QUA-SD_6- 170921/1570
Incorrect Type Conversion or Cast	08-Sep-21	4.6	Incorrect pointer argument passed to trusted application TA could result in un- intended memory operations in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Industrial IOT CVE ID : CVE-2021-1923	https://www. qualcomm.co m/company/ product- security/bull etins/august- 2021-bulletin	H-QUA-SD_6- 170921/1571
Exposure of Resource to Wrong Sphere CVSS Scoring Sc	08-Sep-21	2.1	Lack of strict validation of bootmode can lead to information disclosure in Snapdragon Auto,	https://www. qualcomm.co m/company/ product-	H-QUA-SD_6- 170921/1572 8-9 9-10

Description & CVE ID	Patch	NCIIPC ID						
Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wearables	security/bull etins/august- 2021-bulletin							
CVE ID : CVE-2021-1929								
Possible out of bounds read due to incorrect validation of incoming buffer length in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile CVE ID : CVE-2021-1930	https://www. qualcomm.co m/company/ product- security/bull etins/august- 2021-bulletin	H-QUA-SD_6- 170921/1573						
Possible buffer overflow due to improper validation of device types during P2P search in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Woice & Music, Snapdragon Wired Infrastructure and Networking CVE ID : CVE-2021-1972	https://www. qualcomm.co m/company/ product- security/bull etins/august- 2021-bulletin	H-QUA-SD_6- 170921/1574						
sd_8c								
Child process can leak information from parent process due to numeric pids are getting compared and these pid can be reused in	https://www. qualcomm.co m/company/ product- security/bull	H-QUA-SD_8- 170921/1575						
	information from parent process due to numeric pids are getting compared and	information from parent process due to numeric pids are getting compared and these pid can be reused inqualcomm.co m/company/ product- security/bull2-33-44-55-66-77-8						

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables CVE ID : CVE-2021-1904	etins/august- 2021-bulletin	
Loop with Unreachable Exit Condition ('Infinite Loop')	08-Sep-21	5	Loop with unreachable exit condition may occur due to improper handling of unsupported input in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Voice & Music, Snapdragon Wearables CVE ID : CVE-2021-1914	https://www. qualcomm.co m/company/ product- security/bull etins/august- 2021-bulletin	H-QUA-SD_8- 170921/1576
Out-of- bounds Write	08-Sep-21	Possible buffer underflow due to lack of check for negative indices values when processing user provided input in Snapdragon Auto, Snapdragon Compute,		https://www. qualcomm.co m/company/ product- security/bull etins/august- 2021-bulletin	H-QUA-SD_8- 170921/1577
Integer Underflow (Wrap or	08-Sep-21	10	Integer underflow can occur when the RTCP length is lesser than than the actual	https://www. qualcomm.co m/company/	H-QUA-SD_8- 170921/1578

CVSS Scoring Scale	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10
Page 552 of 1/7/										

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Wraparoun d)			blocks present in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Voice & Music, Snapdragon Wearables CVE ID : CVE-2021-1919	product- security/bull etins/august- 2021-bulletin	
Integer Underflow (Wrap or Wraparoun d)	08-Sep-21	10	Integer underflow can occur due to improper handling of incoming RTCP packets in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Voice & Music, Snapdragon Wearables CVE ID : CVE-2021-1920	https://www. qualcomm.co m/company/ product- security/bull etins/august- 2021-bulletin	H-QUA-SD_8- 170921/1579
Incorrect Type Conversion or Cast	08-Sep-21	4.6	Incorrect pointer argument passed to trusted application TA could result in un- intended memory operations in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Industrial IOT CVE ID : CVE-2021-1923	https://www. qualcomm.co m/company/ product- security/bull etins/august- 2021-bulletin	H-QUA-SD_8- 170921/1580
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	08-Sep-21	10	Possible buffer overflow due to improper validation of device types during P2P search in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT,	https://www. qualcomm.co m/company/ product- security/bull etins/august- 2021-bulletin	H-QUA-SD_8- 170921/1581

0-1

1-2

5-6

6-7

7-8

8-9

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking		
			CVE ID : CVE-2021-1972		
sd_8cx					
Exposure of Resource to Wrong Sphere	08-Sep-21	2.1	Child process can leak information from parent process due to numeric pids are getting compared and these pid can be reused in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wearables CVE ID : CVE-2021-1904	https://www. qualcomm.co m/company/ product- security/bull etins/august- 2021-bulletin	H-QUA-SD_8- 170921/1582
Loop with Unreachable Exit Condition ('Infinite Loop')	08-Sep-21	5	Loop with unreachable exit condition may occur due to improper handling of unsupported input in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Voice & Music, Snapdragon Wearables CVE ID : CVE-2021-1914	https://www. qualcomm.co m/company/ product- security/bull etins/august- 2021-bulletin	H-QUA-SD_8- 170921/1583
Out-of- bounds Write	08-Sep-21	10	Possible buffer underflow due to lack of check for negative indices values when	https://www. qualcomm.co m/company/	H-QUA-SD_8- 170921/1584

Page 555 of 1474

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			processing user provided input in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Voice & Music, Snapdragon Wearables CVE ID : CVE-2021-1916	product- security/bull etins/august- 2021-bulletin	
Integer Underflow (Wrap or Wraparoun d)	08-Sep-21	10	Integer underflow can occur when the RTCP length is lesser than than the actual blocks present in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Voice & Music, Snapdragon Wearables CVE ID : CVE-2021-1919	https://www. qualcomm.co m/company/ product- security/bull etins/august- 2021-bulletin	H-QUA-SD_8- 170921/1585
Integer Underflow (Wrap or Wraparoun d)	08-Sep-21	10	Integer underflow can occur due to improper handling of incoming RTCP packets in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Voice & Music, Snapdragon Wearables CVE ID : CVE-2021-1920	https://www. qualcomm.co m/company/ product- security/bull etins/august- 2021-bulletin	H-QUA-SD_8- 170921/1586
Incorrect Type Conversion or Cast	08-Sep-21	4.6	Incorrect pointer argument passed to trusted application TA could result in un- intended memory operations	https://www. qualcomm.co m/company/ product-	H-QUA-SD_8- 170921/1587
CVSS Scoring Sc	ale 0-1	1-2	2-3 3-4 4-5 5-6	6-7 7-8	8-9 9-10

Page 556 of 1474

Weakness	Publish Date	CVSS	Description	n & CVE ID		Pat	ch	NCII	PC ID
			in Snapdragon Snapdragon Co Snapdragon Co Snapdragon Ine	ompute, onnectivit		security etins/a 2021-b	ugust-		
			CVE ID : CVE-2	2021-192	3				
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	08-Sep-21	10	Possible buffer to improper va device types du search in Snapo Snapdragon Co Snapdragon Co Snapdragon Ind Snapdragon Mo Snapdragon Wo Snapdragon Wo Snapdragon Wo Snapdragon Wo Snapdragon Wo Snapdragon Wo Snapdragon Wo Snapdragon Wo Snapdragon Wo Snapdragon Wo	https:// qualcon m/com produc security etins/a 2021-b	nm.co pany/ t- y/bull ugust-	-	-SD_8- 1/1588		
sm4125									
Exposure of Resource to Wrong Sphere	08-Sep-21	2.1	Child process c information fro process due to are getting com these pid can b Snapdragon Au Snapdragon Co Snapdragon Co Snapdragon Ind Snapdragon Ind Snapdragon Mo Snapdragon Wo Snapdragon Wo	https:// qualcon m/com produc security etins/a 2021-b	nm.co pany/ t- y/bull ugust-	-	I-SM41- 1/1589		
Incorrect Type Conversion	08-Sep-21	4.6	Incorrect point passed to trust TA could result		https://www. qualcomm.co m/company/		-	-SM41- 1/1590	
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 & CVE ID	Patch	NCIIPC ID
or Cast			intended memory operations in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Industrial IOT	product- security/bull etins/august- 2021-bulletin	
			CVE ID : CVE-2021-1923		
Improper Restriction of Operations within the Bounds of a Memory Buffer	08-Sep-21	3.6	Possible out of bounds read due to incorrect validation of incoming buffer length in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile	https://www. qualcomm.co m/company/ product- security/bull etins/august- 2021-bulletin	H-QUA-SM41- 170921/1591
			CVE ID : CVE-2021-1930		
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	08-Sep-21	10	Possible buffer overflow due to improper validation of device types during P2P search in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Woice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking CVE ID : CVE-2021-1972	https://www. qualcomm.co m/company/ product- security/bull etins/august- 2021-bulletin	H-QUA-SM41- 170921/1592
sm6250					
Exposure of Resource to Wrong Sphere	08-Sep-21	2.1	Child process can leak information from parent process due to numeric pids are getting compared and these pid can be reused in Snapdragon Auto,	https://www. qualcomm.co m/company/ product- security/bull etins/august-	H-QUA-SM62- 170921/1593
CVSS Scoring Sc	ale 0-1	1-2	2-3 3-4 4-5 5-6 Page 558 of 1474	6-7 7-8	8-9 9-10

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables	2021-bulletin	
			CVE ID : CVE-2021-1904		
Loop with Unreachable Exit Condition ('Infinite Loop')	08-Sep-21	5	Loop with unreachable exit condition may occur due to improper handling of unsupported input in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Voice & Music, Snapdragon Wearables CVE ID : CVE-2021-1914	https://www. qualcomm.co m/company/ product- security/bull etins/august- 2021-bulletin	H-QUA-SM62- 170921/1594
Out-of- bounds Write	08-Sep-21	10	Possible buffer underflow due to lack of check for negative indices values when processing user provided input in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Voice & Music, Snapdragon Wearables CVE ID : CVE-2021-1916	https://www. qualcomm.co m/company/ product- security/bull etins/august- 2021-bulletin	H-QUA-SM62- 170921/1595
Integer Underflow (Wrap or Wraparoun	08-Sep-21	10	Integer underflow can occur when the RTCP length is lesser than than the actual blocks present in Snapdragon	https://www. qualcomm.co m/company/ product-	H-QUA-SM62- 170921/1596

CVEE Searing Scale	0.1	4.2	2.2	2.4	4 5	FC	C 7	7.0	0.0	0.10
CVSS Scoring Scale	0-1	1-2	2-3	3-4	4-5	5-6	6-7	/-8	8-9	9-10
Page 550 of 1/7/										

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
d)			Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Voice & Music, Snapdragon Wearables	security/bull etins/august- 2021-bulletin	
			CVE ID : CVE-2021-1919		
Integer Underflow (Wrap or Wraparoun d)	08-Sep-21	10	Integer underflow can occur due to improper handling of incoming RTCP packets in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Voice & Music, Snapdragon Wearables CVE ID : CVE-2021-1920	https://www. qualcomm.co m/company/ product- security/bull etins/august- 2021-bulletin	H-QUA-SM62- 170921/1597
Incorrect Type Conversion or Cast	08-Sep-21	4.6	Incorrect pointer argument passed to trusted application TA could result in un- intended memory operations in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Industrial IOT CVE ID : CVE-2021-1923	https://www. qualcomm.co m/company/ product- security/bull etins/august- 2021-bulletin	H-QUA-SM62- 170921/1598
Exposure of Resource to Wrong Sphere	08-Sep-21	2.1	Lack of strict validation of bootmode can lead to information disclosure in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile,	https://www. qualcomm.co m/company/ product- security/bull etins/august- 2021-bulletin	H-QUA-SM62- 170921/1599

1-2

2-3

0-1

4-5

5-6

6-7

7-8

8-9

9-10

Publish Date	CVSS	Description & CVE ID	NCIIPC ID	
		Snapdragon Wearables		
		CVE ID : CVE-2021-1929		
08-Sep-21	3.6	Possible out of bounds read due to incorrect validation of incoming buffer length in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile CVE ID : CVE-2021-1930	https://www. qualcomm.co m/company/ product- security/bull etins/august- 2021-bulletin	H-QUA-SM62- 170921/1600
08-Sep-21	10	Possible buffer overflow due to improper validation of device types during P2P search in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Industrial IOT, Snapdragon Woice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking CVE ID : CVE-2021-1972	https://www. qualcomm.co m/company/ product- security/bull etins/august- 2021-bulletin	H-QUA-SM62- 170921/1601
			L	L
sm6250pExposure of Resource to Wrong Sphere08-Sep-212.1		Child process can leak information from parent process due to numeric pids are getting compared and these pid can be reused in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT,	https://www. qualcomm.co m/company/ product- security/bull etins/august- 2021-bulletin	H-QUA-SM62- 170921/1602
	08-Sep-21	Image: marked biase of the second state of the second s	Image: constraint of the section of	Image: constraint of the second sec

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables CVE ID : CVE-2021-1904		
Loop with Unreachable Exit Condition ('Infinite Loop')	08-Sep-21	5	Loop with unreachable exit condition may occur due to improper handling of unsupported input in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Voice & Music, Snapdragon Wearables CVE ID : CVE-2021-1914	https://www. qualcomm.co m/company/ product- security/bull etins/august- 2021-bulletin	H-QUA-SM62- 170921/1603
Out-of- bounds Write	08-Sep-21	10	Possible buffer underflow due to lack of check for negative indices values when processing user provided input in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Voice & Music, Snapdragon Wearables CVE ID : CVE-2021-1916	https://www. qualcomm.co m/company/ product- security/bull etins/august- 2021-bulletin	H-QUA-SM62- 170921/1604
Integer Underflow (Wrap or Wraparoun d)	08-Sep-21	10	Integer underflow can occur when the RTCP length is lesser than than the actual blocks present in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT,	https://www. qualcomm.co m/company/ product- security/bull etins/august- 2021-bulletin	H-QUA-SM62- 170921/1605

1-2 2-3

0-1

4-5

6-7

5-6

7-8

8-9

9-10

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Snapdragon IoT, Snapdragon Voice & Music, Snapdragon Wearables		
			CVE ID : CVE-2021-1919		
Integer Underflow (Wrap or Wraparoun d)	08-Sep-21	10	Integer underflow can occur due to improper handling of incoming RTCP packets in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Voice & Music, Snapdragon Wearables	https://www. qualcomm.co m/company/ product- security/bull etins/august- 2021-bulletin	H-QUA-SM62- 170921/1606
			CVE ID : CVE-2021-1920		
Improper Restriction of Operations within the Bounds of a Memory Buffer	08-Sep-21	3.6	Possible out of bounds read due to incorrect validation of incoming buffer length in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile CVE ID : CVE-2021-1930	https://www. qualcomm.co m/company/ product- security/bull etins/august- 2021-bulletin	H-QUA-SM62- 170921/1607
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	08-Sep-21	10	Possible buffer overflow due to improper validation of device types during P2P search in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Woice & Music, Snapdragon Wearables, Snapdragon Wired	https://www. qualcomm.co m/company/ product- security/bull etins/august- 2021-bulletin	H-QUA-SM62- 170921/1608

0-1

1-2

7-8

5-6

6-7

8-9

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Infrastructure and Networking		
			CVE ID : CVE-2021-1972		
sm7250			CVE ID : CVE-2021-1972		
5111/250					
Exposure of Resource to Wrong Sphere	08-Sep-21	2.1	Child process can leak information from parent process due to numeric pids are getting compared and these pid can be reused in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wearables CVE ID : CVE-2021-1904	https://www. qualcomm.co m/company/ product- security/bull etins/august- 2021-bulletin	H-QUA-SM72- 170921/1609
Loop with Unreachable Exit Condition ('Infinite Loop')	08-Sep-21	5	Loop with unreachable exit condition may occur due to improper handling of unsupported input in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Voice & Music, Snapdragon Wearables CVE ID : CVE-2021-1914	https://www. qualcomm.co m/company/ product- security/bull etins/august- 2021-bulletin	H-QUA-SM72- 170921/1610
Out-of- bounds Write	08-Sep-21	10	Possible buffer underflow due to lack of check for negative indices values when processing user provided input in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity,	https://www. qualcomm.co m/company/ product- security/bull etins/august- 2021-bulletin	H-QUA-SM72- 170921/1611
CVSS Scoring Sca	ale 0-1	1-2	2-3 3-4 4-5 5-6	6-7 7-8	8-9 9-10

Page 564 of 1474

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Voice & Music, Snapdragon Wearables		
			CVE ID : CVE-2021-1916		
Integer Underflow (Wrap or Wraparoun d)	08-Sep-21	10	Integer underflow can occur when the RTCP length is lesser than than the actual blocks present in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Voice & Music, Snapdragon Wearables	https://www. qualcomm.co m/company/ product- security/bull etins/august- 2021-bulletin	H-QUA-SM72- 170921/1612
			CVE ID : CVE-2021-1919		
Integer Underflow (Wrap or Wraparoun d)	08-Sep-21	10	Integer underflow can occur due to improper handling of incoming RTCP packets in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Voice & Music, Snapdragon Wearables	https://www. qualcomm.co m/company/ product- security/bull etins/august- 2021-bulletin	H-QUA-SM72- 170921/1613
			CVE ID : CVE-2021-1920		
Incorrect Type Conversion or Cast	08-Sep-21	4.6	Incorrect pointer argument passed to trusted application TA could result in un- intended memory operations in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Industrial IOT	https://www. qualcomm.co m/company/ product- security/bull etins/august- 2021-bulletin	H-QUA-SM72- 170921/1614
CVSS Scoring Sca	ale 0-1	1-2		2021-bulletin	8-9 9-1 0

 3-4
 4-5
 5-6

 Page 565 of 1474

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2021-1923		
Exposure of Resource to Wrong Sphere	08-Sep-21	2.1	Lack of strict validation of bootmode can lead to information disclosure in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wearables CVE ID : CVE-2021-1929	https://www. qualcomm.co m/company/ product- security/bull etins/august- 2021-bulletin	H-QUA-SM72- 170921/1615
			Possible out of bounds read		
Improper Restriction of Operations within the Bounds of a Memory Buffer	08-Sep-21	3.6	due to incorrect validation of incoming buffer length in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile CVE ID : CVE-2021-1930	https://www. qualcomm.co m/company/ product- security/bull etins/august- 2021-bulletin	H-QUA-SM72- 170921/1616
			Possible buffer overflow due		
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	08-Sep-21	10	<pre>rossible builler overhow due to improper validation of device types during P2P search in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Woice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking CVE ID : CVE-2021-1972</pre>	https://www. qualcomm.co m/company/ product- security/bull etins/august- 2021-bulletin	H-QUA-SM72- 170921/1617
sm7325					
CVSS Scoring Sc	ale 0-1	1-2	2-3 3-4 4-5 5-6	6-7 7-8	8-9 9-10
			Page 566 of 1474		

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Exposure of Resource to Wrong Sphere	08-Sep-21	2.1	Child process can leak information from parent process due to numeric pids are getting compared and these pid can be reused in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wearables CVE ID : CVE-2021-1904	https://www. qualcomm.co m/company/ product- security/bull etins/august- 2021-bulletin	H-QUA-SM73- 170921/1618
Incorrect Type Conversion or Cast	08-Sep-21	4.6	Incorrect pointer argument passed to trusted application TA could result in un- intended memory operations in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Industrial IOT CVE ID : CVE-2021-1923	https://www. qualcomm.co m/company/ product- security/bull etins/august- 2021-bulletin	H-QUA-SM73- 170921/1619
Exposure of Resource to Wrong Sphere	08-Sep-21	2.1	Lack of strict validation of bootmode can lead to information disclosure in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wearables CVE ID : CVE-2021-1929	https://www. qualcomm.co m/company/ product- security/bull etins/august- 2021-bulletin	H-QUA-SM73- 170921/1620
Improper Restriction of Operations	08-Sep-21	3.6	Possible out of bounds read due to incorrect validation of incoming buffer length in Snapdragon Auto,	https://www. qualcomm.co m/company/ product-	H-QUA-SM73- 170921/1621

CVSS Scoring Scale	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10
			D		64474					

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
within the Bounds of a Memory Buffer			Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile	security/bull etins/august- 2021-bulletin	
			CVE ID : CVE-2021-1930		
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	08-Sep-21	10	Possible buffer overflow due to improper validation of device types during P2P search in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Woice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking CVE ID : CVE-2021-1972	https://www. qualcomm.co m/company/ product- security/bull etins/august- 2021-bulletin	H-QUA-SM73- 170921/1622
wcd9306					
Exposure of Resource to Wrong Sphere	08-Sep-21	2.1	Child process can leak information from parent process due to numeric pids are getting compared and these pid can be reused in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables	https://www. qualcomm.co m/company/ product- security/bull etins/august- 2021-bulletin	H-QUA- WCD9- 170921/1623
			CVE ID : CVE-2021-1904		
Loop with	08-Sep-21	5		https://www.	H-QUA-

 3-4
 4-5
 5-6

 Page 568 of 1474

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Exit Condition ('Infinite Loop')			improper handling of unsupported input in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Voice & Music, Snapdragon Wearables CVE ID : CVE-2021-1914	m/company/ product- security/bull etins/august- 2021-bulletin	170921/1624
Out-of- bounds Write	08-Sep-21	10	Possible buffer underflow due to lack of check for negative indices values when processing user provided input in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Voice & Music, Snapdragon Wearables CVE ID : CVE-2021-1916	https://www. qualcomm.co m/company/ product- security/bull etins/august- 2021-bulletin	H-QUA- WCD9- 170921/1625
Integer Underflow (Wrap or Wraparoun d)	08-Sep-21	10	Integer underflow can occur when the RTCP length is lesser than than the actual blocks present in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Voice & Music, Snapdragon Wearables CVE ID : CVE-2021-1919	https://www. qualcomm.co m/company/ product- security/bull etins/august- 2021-bulletin	H-QUA- WCD9- 170921/1626
Integer Underflow	08-Sep-21	10	Integer underflow can occur due to improper handling of	https://www. qualcomm.co	H-QUA- WCD9-

CVSS Scoring Scale	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10
			Pa	age 569 c	of 1474					

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
(Wrap or Wraparoun d)			incoming RTCP packets in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Voice & Music, Snapdragon Wearables CVE ID : CVE-2021-1920	m/company/ product- security/bull etins/august- 2021-bulletin	170921/1627
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	08-Sep-21	10	Possible buffer overflow due to improper validation of device types during P2P search in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Woice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking CVE ID : CVE-2021-1972	https://www. qualcomm.co m/company/ product- security/bull etins/august- 2021-bulletin	H-QUA- WCD9- 170921/1628
wcd9326					
Exposure of Resource to Wrong Sphere	08-Sep-21	2.1	Child process can leak information from parent process due to numeric pids are getting compared and these pid can be reused in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music,	https://www. qualcomm.co m/company/ product- security/bull etins/august- 2021-bulletin	H-QUA- WCD9- 170921/1629

CVSS Scoring Scale	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10
Page 570 of 1474										

Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
		Snapdragon Wearables		
08-Sep-21	3.6	due to incorrect check of buffer size while flashing emmc devices in Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking	https://www. qualcomm.co m/company/ product- security/bull etins/august- 2021-bulletin	H-QUA- WCD9- 170921/1630
08-Sep-21	2.1	Lack of strict validation of bootmode can lead to information disclosure in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wearables CVE ID : CVE-2021-1929	https://www. qualcomm.co m/company/ product- security/bull etins/august- 2021-bulletin	H-QUA- WCD9- 170921/1631
08-Sep-21	3.6	Possible out of bounds read due to incorrect validation of incoming buffer length in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile CVE ID : CVE-2021-1930	https://www. qualcomm.co m/company/ product- security/bull etins/august- 2021-bulletin	H-QUA- WCD9- 170921/1632
08-Sep-21	10	Possible buffer overflow due to improper validation of	https://www. qualcomm.co	H-QUA- WCD9-
	08-Sep-21 08-Sep-21	• • • •	Image: construct of the second seco	Image: Note of the second se

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Checking Size of Input ('Classic Buffer Overflow')			device types during P2P search in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Woice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking CVE ID : CVE-2021-1972	m/company/ product- security/bull etins/august- 2021-bulletin	170921/1633
wcd9330					
Exposure of Resource to Wrong Sphere	08-Sep-21	2.1	Child process can leak information from parent process due to numeric pids are getting compared and these pid can be reused in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables CVE ID : CVE-2021-1904	https://www. qualcomm.co m/company/ product- security/bull etins/august- 2021-bulletin	H-QUA- WCD9- 170921/1634
Loop with Unreachable Exit Condition ('Infinite Loop')	oop with Inreachable Exit Condition 'Infinite oop')		Loop with unreachable exit condition may occur due to improper handling of unsupported input in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Voice & Music, Snapdragon	https://www. qualcomm.co m/company/ product- security/bull etins/august- 2021-bulletin	H-QUA- WCD9- 170921/1635

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Wearables		
			CVE ID : CVE-2021-1914		
Out-of- bounds Write	08-Sep-21	10	Possible buffer underflow due to lack of check for negative indices values when processing user provided input in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Voice & Music, Snapdragon Wearables	https://www. qualcomm.co m/company/ product- security/bull etins/august- 2021-bulletin	H-QUA- WCD9- 170921/1636
			CVE ID : CVE-2021-1916		
Integer Underflow (Wrap or Wraparoun d)	08-Sep-21	10	Integer underflow can occur when the RTCP length is lesser than than the actual blocks present in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Voice & Music, Snapdragon Wearables CVE ID : CVE-2021-1919	https://www. qualcomm.co m/company/ product- security/bull etins/august- 2021-bulletin	H-QUA- WCD9- 170921/1637
Integer Underflow (Wrap or Wraparoun d)	08-Sep-21	10	Integer underflow can occur due to improper handling of incoming RTCP packets in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Voice & Music, Snapdragon Wearables	https://www. qualcomm.co m/company/ product- security/bull etins/august- 2021-bulletin	H-QUA- WCD9- 170921/1638
CVSS Scoring Sca	ale 0-1	1-2	2-3 3-4 4-5 5-6	6-7 7-8	8-9 9-10

Page 573 of 1474

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2021-1920		
Out-of- bounds Read	08-Sep-21	3.6	Buffer over read could occur due to incorrect check of buffer size while flashing emmc devices in Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking CVE ID : CVE-2021-1928	https://www. qualcomm.co m/company/ product- security/bull etins/august- 2021-bulletin	H-QUA- WCD9- 170921/1639
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	08-Sep-21	10	Possible buffer overflow due to improper validation of device types during P2P search in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Woice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking CVE ID : CVE-2021-1972	https://www. qualcomm.co m/company/ product- security/bull etins/august- 2021-bulletin	H-QUA- WCD9- 170921/1640
wcd9335	I				
Exposure of Resource to Wrong Sphere	08-Sep-21	2.1	Child process can leak information from parent process due to numeric pids are getting compared and these pid can be reused in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity,	https://www. qualcomm.co m/company/ product- security/bull etins/august- 2021-bulletin	H-QUA- WCD9- 170921/1641

0-1

1-2

5-6

6-7

7-8

8-9

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables CVE ID : CVE-2021-1904		
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	08-Sep-21	10	Possible buffer overflow due to improper validation of device types during P2P search in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Industrial IOT, Snapdragon Woice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking CVE ID : CVE-2021-1972	https://www. qualcomm.co m/company/ product- security/bull etins/august- 2021-bulletin	H-QUA- WCD9- 170921/1642
wcd9340					
Exposure of Resource to Wrong Sphere	08-Sep-21	2.1	Child process can leak information from parent process due to numeric pids are getting compared and these pid can be reused in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables	https://www. qualcomm.co m/company/ product- security/bull etins/august- 2021-bulletin	H-QUA- WCD9- 170921/1643
			CVE ID : CVE-2021-1904		
Loop with Unreachable	08-Sep-21	5	CVE ID : CVE-2021-1904 Loop with unreachable exit condition may occur due to	https://www. qualcomm.co	H-QUA- WCD9-

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID	
Exit Condition ('Infinite Loop')			improper handling of unsupported input in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Voice & Music, Snapdragon Wearables CVE ID : CVE-2021-1914	m/company/ product- security/bull etins/august- 2021-bulletin	170921/1644	
Out-of- bounds Write	08-Sep-21	10	Possible buffer underflow due to lack of check for negative indices values when processing user provided input in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Voice & Music, Snapdragon Wearables CVE ID : CVE-2021-1916	https://www. qualcomm.co m/company/ product- security/bull etins/august- 2021-bulletin	H-QUA- WCD9- 170921/1645	
Integer Underflow (Wrap or Wraparoun d)	08-Sep-21	10	Integer underflow can occur when the RTCP length is lesser than than the actual blocks present in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Voice & Music, Snapdragon Wearables CVE ID : CVE-2021-1919	https://www. qualcomm.co m/company/ product- security/bull etins/august- 2021-bulletin	H-QUA- WCD9- 170921/1646	
Integer Underflow	08-Sep-21	10	Integer underflow can occur due to improper handling of	https://www. qualcomm.co	H-QUA- WCD9-	

CVSS Scoring Scale	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10
Page 576 of 1474										

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
(Wrap or Wraparoun d)			incoming RTCP packets in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Voice & Music, Snapdragon Wearables CVE ID : CVE-2021-1920	m/company/ product- security/bull etins/august- 2021-bulletin	170921/1647
Incorrect Type Conversion or Cast	08-Sep-21	4.6	Incorrect pointer argument passed to trusted application TA could result in un- intended memory operations in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Industrial IOT CVE ID : CVE-2021-1923	https://www. qualcomm.co m/company/ product- security/bull etins/august- 2021-bulletin	H-QUA- WCD9- 170921/1648
Out-of- bounds Read	08-Sep-21	3.6	Buffer over read could occur due to incorrect check of buffer size while flashing emmc devices in Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking CVE ID : CVE-2021-1928	https://www. qualcomm.co m/company/ product- security/bull etins/august- 2021-bulletin	H-QUA- WCD9- 170921/1649
Exposure of Resource to Wrong Sphere	08-Sep-21	2.1	Lack of strict validation of bootmode can lead to information disclosure in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity,	https://www. qualcomm.co m/company/ product- security/bull etins/august-	H-QUA- WCD9- 170921/1650

0-1

1-2

5-6

6-7

7-8

8-9

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wearables	2021-bulletin	
			CVE ID : CVE-2021-1929		
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	08-Sep-21	10	Possible buffer overflow due to improper validation of device types during P2P search in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Woice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking CVE ID : CVE-2021-1972	https://www. qualcomm.co m/company/ product- security/bull etins/august- 2021-bulletin	H-QUA- WCD9- 170921/1651
wcd9341					
Exposure of Resource to Wrong Sphere	xposure of esource to rong ohere 08-Sep-21 2.1 Ch in pr ar th Sr Sr Sr Sr Sr Sr Sr Sr Sr Sr Sr Sr Sr		Child process can leak information from parent process due to numeric pids are getting compared and these pid can be reused in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wearables CVE ID : CVE-2021-1904	https://www. qualcomm.co m/company/ product- security/bull etins/august- 2021-bulletin	H-QUA- WCD9- 170921/1652
Exposure of Resource to Wrong	08-Sep-21	2.1	Lack of strict validation of bootmode can lead to information disclosure in	https://www. qualcomm.co m/company/	H-QUA- WCD9- 170921/1653

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Sphere			Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wearables CVE ID : CVE-2021-1929	product- security/bull etins/august- 2021-bulletin	
Improper Restriction of Operations within the Bounds of a Memory Buffer	08-Sep-21	3.6	Possible out of bounds read due to incorrect validation of incoming buffer length in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile CVE ID : CVE-2021-1930	https://www. qualcomm.co m/company/ product- security/bull etins/august- 2021-bulletin	H-QUA- WCD9- 170921/1654
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	08-Sep-21	10	Possible buffer overflow due to improper validation of device types during P2P search in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Woice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking CVE ID : CVE-2021-1972	https://www. qualcomm.co m/company/ product- security/bull etins/august- 2021-bulletin	H-QUA- WCD9- 170921/1655
wcd9360				· 	
Loop with Unreachable Exit Condition	08-Sep-21	5	Loop with unreachable exit condition may occur due to improper handling of unsupported input in	https://www. qualcomm.co m/company/ product-	H-QUA- WCD9- 170921/1656

Page 579 of 1474

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
('Infinite Loop')			Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Voice & Music, Snapdragon Wearables CVE ID : CVE-2021-1914	security/bull etins/august- 2021-bulletin	
Out-of- bounds Write	08-Sep-21	10	Possible buffer underflow due to lack of check for negative indices values when processing user provided input in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Voice & Music, Snapdragon Wearables CVE ID : CVE-2021-1916	https://www. qualcomm.co m/company/ product- security/bull etins/august- 2021-bulletin	H-QUA- WCD9- 170921/1657
Integer Underflow (Wrap or Wraparoun d)	08-Sep-21	10	Integer underflow can occur when the RTCP length is lesser than than the actual blocks present in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Voice & Music, Snapdragon Wearables CVE ID : CVE-2021-1919	https://www. qualcomm.co m/company/ product- security/bull etins/august- 2021-bulletin	H-QUA- WCD9- 170921/1658
Integer Underflow (Wrap or Wraparoun	08-Sep-21	10	Integer underflow can occur due to improper handling of incoming RTCP packets in Snapdragon Auto,	https://www. qualcomm.co m/company/ product-	H-QUA- WCD9- 170921/1659

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
d)			Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Voice & Music, Snapdragon Wearables CVE ID : CVE-2021-1920	security/bull etins/august- 2021-bulletin	
Incorrect Type Conversion or Cast	08-Sep-21	4.6	Incorrect pointer argument passed to trusted application TA could result in un- intended memory operations in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Industrial IOT CVE ID : CVE-2021-1923	https://www. qualcomm.co m/company/ product- security/bull etins/august- 2021-bulletin	H-QUA- WCD9- 170921/1660
wcd9370					
Exposure of Resource to Wrong Sphere	08-Sep-21	2.1	Child process can leak information from parent process due to numeric pids are getting compared and these pid can be reused in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wearables CVE ID : CVE-2021-1904	https://www. qualcomm.co m/company/ product- security/bull etins/august- 2021-bulletin	H-QUA- WCD9- 170921/1661
Loop with Unreachable Exit Condition ('Infinite Loop')	08-Sep-21	5	Loop with unreachable exit condition may occur due to improper handling of unsupported input in Snapdragon Auto, Snapdragon Compute,	https://www. qualcomm.co m/company/ product- security/bull etins/august-	H-QUA- WCD9- 170921/1662

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Voice & Music, Snapdragon Wearables CVE ID : CVE-2021-1914	2021-bulletin	
Out-of- bounds Write	08-Sep-21	10	Possible buffer underflow due to lack of check for negative indices values when processing user provided input in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Voice & Music, Snapdragon Wearables CVE ID : CVE-2021-1916	https://www. qualcomm.co m/company/ product- security/bull etins/august- 2021-bulletin	H-QUA- WCD9- 170921/1663
Integer Underflow (Wrap or Wraparoun d)	08-Sep-21	10	Integer underflow can occur when the RTCP length is lesser than than the actual blocks present in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Voice & Music, Snapdragon Wearables CVE ID : CVE-2021-1919	https://www. qualcomm.co m/company/ product- security/bull etins/august- 2021-bulletin	H-QUA- WCD9- 170921/1664
Integer Underflow (Wrap or Wraparoun d)	08-Sep-21	10	Integer underflow can occur due to improper handling of incoming RTCP packets in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity,	https://www. qualcomm.co m/company/ product- security/bull etins/august-	H-QUA- WCD9- 170921/1665

0-1

1-2

7-8

5-6

6-7

8-9

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Voice & Music, Snapdragon Wearables	2021-bulletin	
			CVE ID : CVE-2021-1920		
Incorrect Type Conversion or Cast	08-Sep-21	4.6	Incorrect pointer argument passed to trusted application TA could result in un- intended memory operations in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Industrial IOT	https://www. qualcomm.co m/company/ product- security/bull etins/august- 2021-bulletin	H-QUA- WCD9- 170921/1666
			CVE ID : CVE-2021-1923		
Exposure of Resource to Wrong Sphere	08-Sep-21	2.1	Lack of strict validation of bootmode can lead to information disclosure in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wearables CVE ID : CVE-2021-1929	https://www. qualcomm.co m/company/ product- security/bull etins/august- 2021-bulletin	H-QUA- WCD9- 170921/1667
Improper Restriction of Operations within the Bounds of a Memory Buffer	08-Sep-21	CVE ID : CVE 2021 1929Possible out of bounds read due to incorrect validation of incoming buffer length in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile CVE ID : CVE-2021-1930		https://www. qualcomm.co m/company/ product- security/bull etins/august- 2021-bulletin	H-QUA- WCD9- 170921/1668
Buffer Copy without	08-Sep-21	10	Possible buffer overflow due to improper validation of	https://www. qualcomm.co	H-QUA- WCD9-

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Checking Size of Input ('Classic Buffer Overflow')			device types during P2P search in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Woice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking CVE ID : CVE-2021-1972	m/company/ product- security/bull etins/august- 2021-bulletin	170921/1669
wcd9371					
Exposure of Resource to Wrong Sphere	08-Sep-21	2.1	Child process can leak information from parent process due to numeric pids are getting compared and these pid can be reused in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables CVE ID : CVE-2021-1904	https://www. qualcomm.co m/company/ product- security/bull etins/august- 2021-bulletin	H-QUA- WCD9- 170921/1670
Loop with Unreachable Exit Condition ('Infinite Loop')		Loop with unreachable exit condition may occur due to improper handling of unsupported input in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Voice & Music, Snapdragon	https://www. qualcomm.co m/company/ product- security/bull etins/august- 2021-bulletin	H-QUA- WCD9- 170921/1671	

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID	
			Wearables			
			CVE ID : CVE-2021-1914			
Out-of- bounds Write	08-Sep-21	10	Possible buffer underflow due to lack of check for negative indices values when processing user provided input in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Voice & Music, Snapdragon Wearables	https://www. qualcomm.co m/company/ product- security/bull etins/august- 2021-bulletin	H-QUA- WCD9- 170921/1672	
			CVE ID : CVE-2021-1916			
Integer Underflow (Wrap or Wraparoun d)	08-Sep-21	10	Integer underflow can occur when the RTCP length is lesser than than the actual blocks present in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Voice & Music, Snapdragon Wearables CVE ID : CVE-2021-1919	https://www. qualcomm.co m/company/ product- security/bull etins/august- 2021-bulletin	H-QUA- WCD9- 170921/1673	
Integer Underflow (Wrap or Wraparoun d)	08-Sep-21	10	Integer underflow can occur due to improper handling of incoming RTCP packets in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Voice & Music, Snapdragon Wearables	https://www. qualcomm.co m/company/ product- security/bull etins/august- 2021-bulletin	H-QUA- WCD9- 170921/1674	
CVSS Scoring Sc	ale 0-1	1-2	2-3 3-4 4-5 5-6	6-7 7-8	8-9 9-10	

Page 585 of 1474

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2021-1920		
Improper Restriction of Operations within the Bounds of a Memory Buffer	08-Sep-21	3.6	Possible out of bounds read due to incorrect validation of incoming buffer length in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile CVE ID : CVE-2021-1930	https://www. qualcomm.co m/company/ product- security/bull etins/august- 2021-bulletin	H-QUA- WCD9- 170921/1675
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	08-Sep-21	10	Possible buffer overflow due to improper validation of device types during P2P search in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Woice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking CVE ID : CVE-2021-1972	https://www. qualcomm.co m/company/ product- security/bull etins/august- 2021-bulletin	H-QUA- WCD9- 170921/1676
wcd9375	I			I	
Exposure of Resource to Wrong Sphere	08-Sep-21	2.1	Child process can leak information from parent process due to numeric pids are getting compared and these pid can be reused in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile,	https://www. qualcomm.co m/company/ product- security/bull etins/august- 2021-bulletin	H-QUA- WCD9- 170921/1677

Г											
	CVSS Scoring Scale	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Snapdragon Voice & Music, Snapdragon Wearables		
			CVE ID : CVE-2021-1904		
Loop with Unreachable Exit Condition ('Infinite Loop')	08-Sep-21	5	Loop with unreachable exit condition may occur due to improper handling of unsupported input in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Voice & Music, Snapdragon Wearables CVE ID : CVE-2021-1914	https://www. qualcomm.co m/company/ product- security/bull etins/august- 2021-bulletin	H-QUA- WCD9- 170921/1678
Out-of- bounds Write	08-Sep-21	10	Possible buffer underflow due to lack of check for negative indices values when processing user provided input in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Voice & Music, Snapdragon Wearables CVE ID : CVE-2021-1916	https://www. qualcomm.co m/company/ product- security/bull etins/august- 2021-bulletin	H-QUA- WCD9- 170921/1679
Integer Underflow (Wrap or Wraparoun d)	08-Sep-21	10	Integer underflow can occur when the RTCP length is lesser than than the actual blocks present in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon	https://www. qualcomm.co m/company/ product- security/bull etins/august- 2021-bulletin	H-QUA- WCD9- 170921/1680

1-2

0-1

5-6

6-7

7-8

8-9

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Voice & Music, Snapdragon Wearables CVE ID : CVE-2021-1919		
Integer Underflow (Wrap or Wraparoun d)	08-Sep-21	10	Integer underflow can occur due to improper handling of incoming RTCP packets in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Voice & Music, Snapdragon Wearables	https://www. qualcomm.co m/company/ product- security/bull etins/august- 2021-bulletin	H-QUA- WCD9- 170921/1681
			CVE ID : CVE-2021-1920		
Incorrect Type Conversion or Cast	08-Sep-21	4.6	Incorrect pointer argument passed to trusted application TA could result in un- intended memory operations in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Industrial IOT CVE ID : CVE-2021-1923	https://www. qualcomm.co m/company/ product- security/bull etins/august- 2021-bulletin	H-QUA- WCD9- 170921/1682
Exposure of Resource to Wrong Sphere	08-Sep-21	2.1	Lack of strict validation of bootmode can lead to information disclosure in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wearables CVE ID : CVE-2021-1929	https://www. qualcomm.co m/company/ product- security/bull etins/august- 2021-bulletin	H-QUA- WCD9- 170921/1683
Improper Restriction of	08-Sep-21	3.6	Possible out of bounds read due to incorrect validation of incoming buffer length in	https://www. qualcomm.co m/company/	H-QUA- WCD9-
CVSS Scoring Sc	ale 0-1	1-2	2-3 3-4 4-5 5-6	6-7 7-8	8-9 9-10

Operations within the Bounds of a Memory BufferIsaparagon Campute, Snapdragon Compute, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Industrial IOT, Snapdragon Industrial IOT, Snapdragon Industrial IOT, Snapdragon Industrial IOT, Snapdragon Consumer IOT, Snapdragon Notice & Music, Snapdragon Notice & Music, Snapdragon Vice & Music, Snapdragon Noice & Music, Snapdragon Consumer IOT, Snapdragon Consumer IOT, Snapdragon Vice & Music, Snapdragon Consumer IOT, Snapdragon Consumer IOT, Snapdragon Consumer IOT, Snapdragon Consumer IOT, Snapdragon Consumer IOT, Snapdragon Auto, Snapdragon Consumer IOT, Snapdragon Neice & Music, Snapdragon Neice & Music, Snapdragon Neice	Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Buffer Copy without Checking Size of Input (Classic Overflow')08-Sep-21Passible buffer overflow due to improper validation of device types during P2P search in Snapdragon Compute, Snapdragon Connectivity, Snapdragon Connectivity, Snapdragon Industrial I0T, Snapdragon Nobile, Snapdragon Nobile, Snapdragon Wearables, Snapdragon Consumer I0T, Snapdragon Mobile, Snapdragon Mobile, Snapdragon Consumer I0T, Snapdragon Mobile, Snapdragon Consumer I0T, Snapdragon Consumer I0T, <td>within the Bounds of a Memory</td> <td></td> <td></td> <td>Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT,</td> <td>security/bull etins/august-</td> <td>170921/1684</td>	within the Bounds of a Memory			Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT,	security/bull etins/august-	170921/1684
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')08-Sep-21III <th< td=""><td></td><td></td><td></td><td>CVE ID : CVE-2021-1930</td><td></td><td></td></th<>				CVE ID : CVE-2021-1930		
Exposure of Resource to Wrong Sphere08-Sep-212.1Child process can leak 	without Checking Size of Input ('Classic Buffer	08-Sep-21	10	to improper validation of device types during P2P search in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Woice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking	qualcomm.co m/company/ product- security/bull etins/august-	WCD9-
Exposure of Resource to Wrong Sphere08-Sep-212.1Information from parent process due to numeric pids are getting compared and these pid can be reused in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wearableshttps://www. qualcomm.co m/company/ product- security/bull etins/august- 2021-bulletinH-QUA- WCD9- 170921/1686	wcd9380					
Loop with08-Sep-215Loop with unreachable exithttps://www.H-QUA-	Resource to Wrong	08-Sep-21	2.1	information from parent process due to numeric pids are getting compared and these pid can be reused in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wearables	qualcomm.co m/company/ product- security/bull etins/august-	WCD9-
	Loop with	08-Sep-21	5	Loop with unreachable exit	https://www.	H-QUA-

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID		
Unreachable Exit Condition ('Infinite Loop')			condition may occur due to improper handling of unsupported input in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Voice & Music, Snapdragon Wearables	qualcomm.co m/company/ product- security/bull etins/august- 2021-bulletin	WCD9- 170921/1687		
			CVE ID : CVE-2021-1914				
Out-of- bounds Write	08-Sep-21	10	Possible buffer underflow due to lack of check for negative indices values when processing user provided input in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Voice & Music, Snapdragon Wearables	https://www. qualcomm.co m/company/ product- security/bull etins/august- 2021-bulletin	H-QUA- WCD9- 170921/1688		
			CVE ID : CVE-2021-1916				
Integer Underflow (Wrap or Wraparoun d)	08-Sep-21	10	Integer underflow can occur when the RTCP length is lesser than than the actual blocks present in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Voice & Music, Snapdragon Wearables	https://www. qualcomm.co m/company/ product- security/bull etins/august- 2021-bulletin	H-QUA- WCD9- 170921/1689		
	00 6 - 21	10	CVE ID : CVE-2021-1919				
Integer 08-Sep-21 10 Integer underflow can occur https://www. H-QUA-							

 3-4
 4-5
 5-6

 Page 590 of 1474

		due to improper handling of incoming RTCP packets in	qualcomm.co	WCD9-
		Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Voice & Music, Snapdragon Wearables CVE ID : CVE-2021-1920	m/company/ product- security/bull etins/august- 2021-bulletin	170921/1690
08-Sep-21	4.6	Incorrect pointer argument passed to trusted application TA could result in un- intended memory operations in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Industrial IOT CVE ID : CVE-2021-1923	https://www. qualcomm.co m/company/ product- security/bull etins/august- 2021-bulletin	H-QUA- WCD9- 170921/1691
08-Sep-21	2.1	Lack of strict validation of bootmode can lead to information disclosure in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wearables CVE ID : CVE-2021-1929	https://www. qualcomm.co m/company/ product- security/bull etins/august- 2021-bulletin	H-QUA- WCD9- 170921/1692
08-Sep-21	3.6	Possible out of bounds read due to incorrect validation of incoming buffer length in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT,	https://www. qualcomm.co m/company/ product- security/bull etins/august- 2021-bulletin	H-QUA- WCD9- 170921/1693
	08-Sep-21	08-Sep-21 2.1 08-Sep-21 3.6	Snapdragon IoT, Snapdragon Voice & Music, Snapdragon WearablesCVE ID : CVE-2021-192008-Sep-21Incorrect pointer argument passed to trusted application TA could result in un- intended memory operations in Snapdragon Auto, Snapdragon Compute, Snapdragon Industrial IOT CVE ID : CVE-2021-192308-Sep-21Image: Image: I	Image: Second

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Buffer			Snapdragon Industrial IOT, Snapdragon Mobile CVE ID : CVE-2021-1930		
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	08-Sep-21	10	Possible buffer overflow due to improper validation of device types during P2P search in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Woice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking CVE ID : CVE-2021-1972	https://www. qualcomm.co m/company/ product- security/bull etins/august- 2021-bulletin	H-QUA- WCD9- 170921/1694
wcd9385	I			L	L
Exposure of Resource to Wrong Sphere	08-Sep-21	2.1	Child process can leak information from parent process due to numeric pids are getting compared and these pid can be reused in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wearables CVE ID : CVE-2021-1904	https://www. qualcomm.co m/company/ product- security/bull etins/august- 2021-bulletin	H-QUA- WCD9- 170921/1695
Loop with Unreachable Exit Condition ('Infinite	08-Sep-21	5	Loop with unreachable exit condition may occur due to improper handling of unsupported input in Snapdragon Auto,	https://www. qualcomm.co m/company/ product- security/bull	H-QUA- WCD9- 170921/1696
CVSS Scoring Sc	ale 0-1	1-2	2-3 3-4 4-5 5-6	6-7 7-8	8-9 9-10

Page 592 of 1474

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Loop')			Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Voice & Music, Snapdragon Wearables CVE ID : CVE-2021-1914	etins/august- 2021-bulletin	
Out-of- bounds Write	08-Sep-21	10	Possible buffer underflow due to lack of check for negative indices values when processing user provided input in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Voice & Music, Snapdragon Wearables CVE ID : CVE-2021-1916	https://www. qualcomm.co m/company/ product- security/bull etins/august- 2021-bulletin	H-QUA- WCD9- 170921/1697
Integer Underflow (Wrap or Wraparoun d)	08-Sep-21	10	Integer underflow can occur when the RTCP length is lesser than than the actual blocks present in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Voice & Music, Snapdragon Wearables CVE ID : CVE-2021-1919	https://www. qualcomm.co m/company/ product- security/bull etins/august- 2021-bulletin	H-QUA- WCD9- 170921/1698
Integer Underflow (Wrap or Wraparoun d)	08-Sep-21	10	Integer underflow can occur due to improper handling of incoming RTCP packets in Snapdragon Auto, Snapdragon Compute,	https://www. qualcomm.co m/company/ product- security/bull	H-QUA- WCD9- 170921/1699
CVSS Scoring Sco	ale 0-1	1-2	2-3 3-4 4-5 5-6	6-7 7-8	8-9 9-10

3-4 4-5 Page 593 of 1474

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Voice & Music, Snapdragon Wearables	etins/august- 2021-bulletin	
			CVE ID : CVE-2021-1920		
Incorrect Type Conversion or Cast	08-Sep-21	4.6	Incorrect pointer argument passed to trusted application TA could result in un- intended memory operations in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Industrial IOT CVE ID : CVE-2021-1923	https://www. qualcomm.co m/company/ product- security/bull etins/august- 2021-bulletin	H-QUA- WCD9- 170921/1700
Exposure of Resource to Wrong Sphere	08-Sep-21	2.1	Lack of strict validation of bootmode can lead to information disclosure in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wearables CVE ID : CVE-2021-1929	https://www. qualcomm.co m/company/ product- security/bull etins/august- 2021-bulletin	H-QUA- WCD9- 170921/1701
Improper Restriction of Operations within the Bounds of a Memory Buffer	08-Sep-21	3.6	Possible out of bounds read due to incorrect validation of incoming buffer length in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile CVE ID : CVE-2021-1930	https://www. qualcomm.co m/company/ product- security/bull etins/august- 2021-bulletin	H-QUA- WCD9- 170921/1702

CVSS Scoring Scale	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10
			P	age 594 c	of 1474					

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	08-Sep-21	10	Possible buffer overflow due to improper validation of device types during P2P search in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Woice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking CVE ID : CVE-2021-1972	https://www. qualcomm.co m/company/ product- security/bull etins/august- 2021-bulletin	H-QUA- WCD9- 170921/1703
wcn3610					·
Exposure of Resource to Wrong Sphere	08-Sep-21	2.1	Child process can leak information from parent process due to numeric pids are getting compared and these pid can be reused in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wearables CVE ID : CVE-2021-1904	https://www. qualcomm.co m/company/ product- security/bull etins/august- 2021-bulletin	H-QUA- WCN3- 170921/1704
Loop with Unreachable Exit Condition ('Infinite Loop')	08-Sep-21	5	Loop with unreachable exit condition may occur due to improper handling of unsupported input in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT,	https://www. qualcomm.co m/company/ product- security/bull etins/august- 2021-bulletin	H-QUA- WCN3- 170921/1705

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Snapdragon IoT, Snapdragon Voice & Music, Snapdragon Wearables		
			CVE ID : CVE-2021-1914		
Out-of- bounds Write	08-Sep-21	10	Possible buffer underflow due to lack of check for negative indices values when processing user provided input in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Voice & Music, Snapdragon Wearables	https://www. qualcomm.co m/company/ product- security/bull etins/august- 2021-bulletin	H-QUA- WCN3- 170921/1706
Integer Underflow (Wrap or Wraparoun d)	08-Sep-21	10	CVE ID : CVE-2021-1916 Integer underflow can occur when the RTCP length is lesser than than the actual blocks present in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Voice & Music, Snapdragon Wearables	https://www. qualcomm.co m/company/ product- security/bull etins/august- 2021-bulletin	H-QUA- WCN3- 170921/1707
			CVE ID : CVE-2021-1919		
Integer Underflow (Wrap or Wraparoun d)	08-Sep-21	10	Integer underflow can occur due to improper handling of incoming RTCP packets in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon	https://www. qualcomm.co m/company/ product- security/bull etins/august- 2021-bulletin	H-QUA- WCN3- 170921/1708

1-2

0-1

5-6

6-7

7-8

8-9

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Voice & Music, Snapdragon Wearables		
			CVE ID : CVE-2021-1920		
Out-of- bounds Read	08-Sep-21	3.6	Buffer over read could occur due to incorrect check of buffer size while flashing emmc devices in Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking CVE ID : CVE-2021-1928	https://www. qualcomm.co m/company/ product- security/bull etins/august- 2021-bulletin	H-QUA- WCN3- 170921/1709
Exposure of Resource to Wrong Sphere	08-Sep-21	2.1	Lack of strict validation of bootmode can lead to information disclosure in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wearables CVE ID : CVE-2021-1929	https://www. qualcomm.co m/company/ product- security/bull etins/august- 2021-bulletin	H-QUA- WCN3- 170921/1710
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	08-Sep-21	10	Possible buffer overflow due to improper validation of device types during P2P search in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables,	https://www. qualcomm.co m/company/ product- security/bull etins/august- 2021-bulletin	H-QUA- WCN3- 170921/1711

0-1

1-2 2-3 4-5

5-6

6-7

7-8

8-9

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Snapdragon Wired Infrastructure and Networking		
			CVE ID : CVE-2021-1972		
wcn3615					
Exposure of Resource to Wrong Sphere	08-Sep-21	2.1	Child process can leak information from parent process due to numeric pids are getting compared and these pid can be reused in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wearables CVE ID : CVE-2021-1904	https://www. qualcomm.co m/company/ product- security/bull etins/august- 2021-bulletin	H-QUA- WCN3- 170921/1712
Loop with Unreachable Exit Condition ('Infinite Loop')	08-Sep-21	5	Loop with unreachable exit condition may occur due to improper handling of unsupported input in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Voice & Music, Snapdragon Wearables CVE ID : CVE-2021-1914	https://www. qualcomm.co m/company/ product- security/bull etins/august- 2021-bulletin	H-QUA- WCN3- 170921/1713
Out-of- bounds Write	08-Sep-21	10	Possible buffer underflow due to lack of check for negative indices values when processing user provided input in Snapdragon Auto, Snapdragon Compute,	https://www. qualcomm.co m/company/ product- security/bull etins/august-	H-QUA- WCN3- 170921/1714
CVSS Scoring Sc	ale 0-1	1-2	2-3 3-4 4-5 5-6	6-7 7-8	8-9 9-10

Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
		Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Voice & Music, Snapdragon Wearables	2021-bulletin	
		CVE ID : CVE-2021-1916		
08-Sep-21	10	Integer underflow can occur when the RTCP length is lesser than than the actual blocks present in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Voice & Music, Snapdragon Wearables	https://www. qualcomm.co m/company/ product- security/bull etins/august- 2021-bulletin	H-QUA- WCN3- 170921/1715
		CVE ID : CVE-2021-1919		
08-Sep-21	10	Integer underflow can occur due to improper handling of incoming RTCP packets in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Voice & Music, Snapdragon Wearables CVE ID : CVE-2021-1920	https://www. qualcomm.co m/company/ product- security/bull etins/august- 2021-bulletin	H-QUA- WCN3- 170921/1716
08-Sep-21	2.1	Lack of strict validation of bootmode can lead to information disclosure in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT,	https://www. qualcomm.co m/company/ product- security/bull etins/august- 2021-bulletin	H-QUA- WCN3- 170921/1717
	08-Sep-21	08-Sep-21 10 08-Sep-21 10	Image: construct of the second seco	08-Sep-21110Snapdragon Connectivity, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Voice & Music, Snapdragon Wearables2021-bulletin08-Sep-21110Integer underflow can occur when the RTCP length is lesser than than the actual blocks present in Snapdragon Auto, Snapdragon Connectivity, Snapdragon IoT, Snapdragon Auto, Snapdragon Consumer IOT, Snapdragon Consumer IOT, Snapdragon Consumer IOT, Snapdragon Consumer IOT, Snapdragon IoT, Snapdragon Auto, Snapdragon Consumer IOT, Snapdragon IoT, Snapdragon Voice & Music, Snapdragon Voice & Mu

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wearables		
			CVE ID : CVE-2021-1929		
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	08-Sep-21	10	Possible buffer overflow due to improper validation of device types during P2P search in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Woice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking CVE ID : CVE-2021-1972	https://www. qualcomm.co m/company/ product- security/bull etins/august- 2021-bulletin	H-QUA- WCN3- 170921/1718
wcn3620					
Exposure of Resource to Wrong Sphere	08-Sep-21	2.1	Child process can leak information from parent process due to numeric pids are getting compared and these pid can be reused in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wearables CVE ID : CVE-2021-1904	https://www. qualcomm.co m/company/ product- security/bull etins/august- 2021-bulletin	H-QUA- WCN3- 170921/1719
Loop with Unreachable Exit Condition	08-Sep-21	5	Loop with unreachable exit condition may occur due to improper handling of unsupported input in	https://www. qualcomm.co m/company/ product-	H-QUA- WCN3- 170921/1720
CVSS Scoring Sc	ale 0-1	1-2	2-3 3-4 4-5 5-6	6-7 7-8	8-9 9-10

Page 600 of 1474

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
('Infinite Loop')			Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Voice & Music, Snapdragon Wearables CVE ID : CVE-2021-1914	security/bull etins/august- 2021-bulletin	
Out-of- bounds Write	08-Sep-21	10	Possible buffer underflow due to lack of check for negative indices values when processing user provided input in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Voice & Music, Snapdragon Wearables CVE ID : CVE-2021-1916	https://www. qualcomm.co m/company/ product- security/bull etins/august- 2021-bulletin	H-QUA- WCN3- 170921/1721
Integer Underflow (Wrap or Wraparoun d)	08-Sep-21	10	Integer underflow can occur when the RTCP length is lesser than than the actual blocks present in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Voice & Music, Snapdragon Wearables CVE ID : CVE-2021-1919	https://www. qualcomm.co m/company/ product- security/bull etins/august- 2021-bulletin	H-QUA- WCN3- 170921/1722
Integer Underflow (Wrap or Wraparoun	08-Sep-21	10	Integer underflow can occur due to improper handling of incoming RTCP packets in Snapdragon Auto,	https://www. qualcomm.co m/company/ product-	H-QUA- WCN3- 170921/1723

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
d)			Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Voice & Music, Snapdragon Wearables	security/bull etins/august- 2021-bulletin	
			CVE ID : CVE-2021-1920		
Out-of- bounds Read	08-Sep-21	3.6	Buffer over read could occur due to incorrect check of buffer size while flashing emmc devices in Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking CVE ID : CVE-2021-1928	https://www. qualcomm.co m/company/ product- security/bull etins/august- 2021-bulletin	H-QUA- WCN3- 170921/1724
Exposure of Resource to Wrong Sphere	08-Sep-21	2.1	Lack of strict validation of bootmode can lead to information disclosure in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wearables CVE ID : CVE-2021-1929	https://www. qualcomm.co m/company/ product- security/bull etins/august- 2021-bulletin	H-QUA- WCN3- 170921/1725
Buffer Copy without Checking Size of Input ('Classic Buffer	08-Sep-21	10	Possible buffer overflow due to improper validation of device types during P2P search in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity,	https://www. qualcomm.co m/company/ product- security/bull etins/august-	H-QUA- WCN3- 170921/1726

0-1

1-2

4-5

6-7

5-6

7-8

8-9

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Overflow')			Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking CVE ID : CVE-2021-1972	2021-bulletin	
wcn3660					
Exposure of Resource to Wrong Sphere	08-Sep-21	2.1	Child process can leak information from parent process due to numeric pids are getting compared and these pid can be reused in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables CVE ID : CVE-2021-1904	https://www. qualcomm.co m/company/ product- security/bull etins/august- 2021-bulletin	H-QUA- WCN3- 170921/1727
Loop with Unreachable Exit Condition ('Infinite Loop')	08-Sep-21	5	Loop with unreachable exit condition may occur due to improper handling of unsupported input in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Voice & Music, Snapdragon Wearables CVE ID : CVE-2021-1914	https://www. qualcomm.co m/company/ product- security/bull etins/august- 2021-bulletin	H-QUA- WCN3- 170921/1728
Out-of-	08-Sep-21	10	Possible buffer underflow	https://www.	H-QUA-
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 & CVE ID	Patch	NCIIPC ID
bounds Write			due to lack of check for negative indices values when processing user provided input in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Voice & Music, Snapdragon Wearables CVE ID : CVE-2021-1916	qualcomm.co m/company/ product- security/bull etins/august- 2021-bulletin	WCN3- 170921/1729
			Integer underflow can occur		
Integer Underflow (Wrap or Wraparoun d)	08-Sep-21	10	when the RTCP length is lesser than than the actual blocks present in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Voice & Music, Snapdragon Wearables	https://www. qualcomm.co m/company/ product- security/bull etins/august- 2021-bulletin	H-QUA- WCN3- 170921/1730
			CVE ID : CVE-2021-1919		
Integer Underflow (Wrap or Wraparoun d)	08-Sep-21	10	Integer underflow can occur due to improper handling of incoming RTCP packets in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Voice & Music, Snapdragon Wearables	https://www. qualcomm.co m/company/ product- security/bull etins/august- 2021-bulletin	H-QUA- WCN3- 170921/1731
			CVE ID : CVE-2021-1920		
Buffer Copy without	08-Sep-21	10	Possible buffer overflow due to improper validation of	https://www. qualcomm.co	H-QUA- WCN3-

CVSS Scoring Scale	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10
Page 604 of 1474										

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Checking Size of Input ('Classic Buffer Overflow')			device types during P2P search in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Woice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking CVE ID : CVE-2021-1972	m/company/ product- security/bull etins/august- 2021-bulletin	170921/1732
wcn3660b					
Exposure of Resource to Wrong Sphere	08-Sep-21	2.1	Child process can leak information from parent process due to numeric pids are getting compared and these pid can be reused in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables CVE ID : CVE-2021-1904	https://www. qualcomm.co m/company/ product- security/bull etins/august- 2021-bulletin	H-QUA- WCN3- 170921/1733
Loop with Unreachable Exit Condition ('Infinite Loop')	08-Sep-21	5	Loop with unreachable exit condition may occur due to improper handling of unsupported input in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Voice & Music, Snapdragon	https://www. qualcomm.co m/company/ product- security/bull etins/august- 2021-bulletin	H-QUA- WCN3- 170921/1734

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Wearables		
			CVE ID : CVE-2021-1914		
Out-of- bounds Write	08-Sep-21	10	Possible buffer underflow due to lack of check for negative indices values when processing user provided input in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Voice & Music, Snapdragon Wearables	https://www. qualcomm.co m/company/ product- security/bull etins/august- 2021-bulletin	H-QUA- WCN3- 170921/1735
			CVE ID : CVE-2021-1916		
Integer Underflow (Wrap or Wraparoun d)	08-Sep-21	10	Integer underflow can occur when the RTCP length is lesser than than the actual blocks present in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Voice & Music, Snapdragon Wearables CVE ID : CVE-2021-1919	https://www. qualcomm.co m/company/ product- security/bull etins/august- 2021-bulletin	H-QUA- WCN3- 170921/1736
Integer Underflow (Wrap or Wraparoun d)	08-Sep-21	10	Integer underflow can occur due to improper handling of incoming RTCP packets in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Voice & Music, Snapdragon Wearables	https://www. qualcomm.co m/company/ product- security/bull etins/august- 2021-bulletin	H-QUA- WCN3- 170921/1737
CVSS Scoring Sc	ale 0-1	1-2	2-3 3-4 4-5 5-6	6-7 7-8	8-9 <mark>9-10</mark>

 3-4
 4-5

 Page 606 of 1474

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2021-1920		
Out-of- bounds Read	08-Sep-21	3.6	Buffer over read could occur due to incorrect check of buffer size while flashing emmc devices in Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking CVE ID : CVE-2021-1928	https://www. qualcomm.co m/company/ product- security/bull etins/august- 2021-bulletin	H-QUA- WCN3- 170921/1738
Exposure of Resource to Wrong Sphere	08-Sep-21	2.1	Lack of strict validation of bootmode can lead to information disclosure in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wearables CVE ID : CVE-2021-1929	https://www. qualcomm.co m/company/ product- security/bull etins/august- 2021-bulletin	H-QUA- WCN3- 170921/1739
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	08-Sep-21	10	Possible buffer overflow due to improper validation of device types during P2P search in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Woice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and	https://www. qualcomm.co m/company/ product- security/bull etins/august- 2021-bulletin	H-QUA- WCN3- 170921/1740

CVSS Scoring Scale	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10
			P	age 607 c	of 1474					

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID		
			Networking				
			CVE ID : CVE-2021-1972				
wcn3680							
Exposure of Resource to Wrong Sphere	08-Sep-21	2.1	Child process can leak information from parent process due to numeric pids are getting compared and these pid can be reused in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wearables CVE ID : CVE-2021-1904	https://www. qualcomm.co m/company/ product- security/bull etins/august- 2021-bulletin	H-QUA- WCN3- 170921/1741		
Loop with Unreachable Exit Condition ('Infinite Loop')	08-Sep-21	5	Loop with unreachable exit condition may occur due to improper handling of unsupported input in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Voice & Music, Snapdragon Wearables CVE ID : CVE-2021-1914	https://www. qualcomm.co m/company/ product- security/bull etins/august- 2021-bulletin	H-QUA- WCN3- 170921/1742		
Out-of- bounds Write	08-Sep-21	10	Possible buffer underflow due to lack of check for negative indices values when processing user provided input in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT,	https://www. qualcomm.co m/company/ product- security/bull etins/august- 2021-bulletin	H-QUA- WCN3- 170921/1743		
CVSS Scoring Scale 0-1 1-2 2-3 3-4 4-5 5-6 6-7 7-8 8-9 9-10							

Page 608 of 1474

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Voice & Music, Snapdragon Wearables		
			CVE ID : CVE-2021-1916		
Integer Underflow (Wrap or Wraparoun d)	08-Sep-21	10	Integer underflow can occur when the RTCP length is lesser than than the actual blocks present in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Voice & Music, Snapdragon Wearables	https://www. qualcomm.co m/company/ product- security/bull etins/august- 2021-bulletin	H-QUA- WCN3- 170921/1744
			CVE ID : CVE-2021-1919		
Integer Underflow (Wrap or Wraparoun d)	08-Sep-21	10	Integer underflow can occur due to improper handling of incoming RTCP packets in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Voice & Music, Snapdragon Wearables	https://www. qualcomm.co m/company/ product- security/bull etins/august- 2021-bulletin	H-QUA- WCN3- 170921/1745
			CVE ID : CVE-2021-1920		
Exposure of Resource to Wrong Sphere	08-Sep-21	2.1	Lack of strict validation of bootmode can lead to information disclosure in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile,	https://www. qualcomm.co m/company/ product- security/bull etins/august- 2021-bulletin	H-QUA- WCN3- 170921/1746

1-2

2-3

0-1

5-6

6-7

7-8

8-9

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID		
			Snapdragon Wearables				
			CVE ID : CVE-2021-1929				
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	08-Sep-21	10	Possible buffer overflow due to improper validation of device types during P2P search in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Woice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking CVE ID : CVE-2021-1972	https://www. qualcomm.co m/company/ product- security/bull etins/august- 2021-bulletin	H-QUA- WCN3- 170921/1747		
wcn3680b							
Exposure of Resource to Wrong Sphere	08-Sep-21	2.1	Child process can leak information from parent process due to numeric pids are getting compared and these pid can be reused in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables CVE ID : CVE-2021-1904	https://www. qualcomm.co m/company/ product- security/bull etins/august- 2021-bulletin	H-QUA- WCN3- 170921/1748		
Loop with Unreachable Exit Condition ('Infinite Loop')	08-Sep-21	5	Loop with unreachable exit condition may occur due to improper handling of unsupported input in Snapdragon Auto, Snapdragon Compute,	https://www. qualcomm.co m/company/ product- security/bull etins/august-	H-QUA- WCN3- 170921/1749		
CVSS Scoring Scale 0-1 1-2 2-3 3-4 4-5 5-6 6-7 7-8 8-9 9-10 Page 610 of 1474							

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Voice & Music, Snapdragon Wearables CVE ID : CVE-2021-1914	2021-bulletin	
Out-of- bounds Write	08-Sep-21	10	Possible buffer underflow due to lack of check for negative indices values when processing user provided input in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Voice & Music, Snapdragon Wearables CVE ID : CVE-2021-1916	https://www. qualcomm.co m/company/ product- security/bull etins/august- 2021-bulletin	H-QUA- WCN3- 170921/1750
Integer Underflow (Wrap or Wraparoun d)	08-Sep-21	10	Integer underflow can occur when the RTCP length is lesser than than the actual blocks present in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Voice & Music, Snapdragon Wearables CVE ID : CVE-2021-1919	https://www. qualcomm.co m/company/ product- security/bull etins/august- 2021-bulletin	H-QUA- WCN3- 170921/1751
Integer Underflow (Wrap or Wraparoun d)	08-Sep-21	10	Integer underflow can occur due to improper handling of incoming RTCP packets in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity,	https://www. qualcomm.co m/company/ product- security/bull etins/august-	H-QUA- WCN3- 170921/1752

0-1

1-2

7-8

5-6

6-7

8-9

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID		
			Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Voice & Music, Snapdragon Wearables	2021-bulletin			
			CVE ID : CVE-2021-1920				
Out-of- bounds Read	08-Sep-21	3.6	Buffer over read could occur due to incorrect check of buffer size while flashing emmc devices in Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking CVE ID : CVE-2021-1928	https://www. qualcomm.co m/company/ product- security/bull etins/august- 2021-bulletin	H-QUA- WCN3- 170921/1753		
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	08-Sep-21	10	Possible buffer overflow due to improper validation of device types during P2P search in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Woice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking CVE ID : CVE-2021-1972	https://www. qualcomm.co m/company/ product- security/bull etins/august- 2021-bulletin	H-QUA- WCN3- 170921/1754		
wcn3910							
Exposure of Resource to Wrong	08-Sep-21	2.1	Child process can leak information from parent process due to numeric pids	https://www. qualcomm.co m/company/	H-QUA- WCN3- 170921/1755		
CVSS Scoring Scale 0-1 1-2 2-3 3-4 4-5 5-6 6-7 7-8 8-9 9-10 Page 612 of 1474							

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Sphere			are getting compared and these pid can be reused in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wearables CVE ID : CVE-2021-1904	product- security/bull etins/august- 2021-bulletin	
Loop with Unreachable Exit Condition ('Infinite Loop')	08-Sep-21	5	Loop with unreachable exit condition may occur due to improper handling of unsupported input in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Voice & Music, Snapdragon Wearables CVE ID : CVE-2021-1914	https://www. qualcomm.co m/company/ product- security/bull etins/august- 2021-bulletin	H-QUA- WCN3- 170921/1756
Out-of- bounds Write	08-Sep-21	10	Possible buffer underflow due to lack of check for negative indices values when processing user provided input in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Voice & Music, Snapdragon Wearables CVE ID : CVE-2021-1916	https://www. qualcomm.co m/company/ product- security/bull etins/august- 2021-bulletin	H-QUA- WCN3- 170921/1757
Integer	08-Sep-21	10	Integer underflow can occur	https://www.	H-QUA-

Page 613 of 1474

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Underflow (Wrap or Wraparoun d)			when the RTCP length is lesser than than the actual blocks present in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Voice & Music, Snapdragon Wearables CVE ID : CVE-2021-1919	qualcomm.co m/company/ product- security/bull etins/august- 2021-bulletin	WCN3- 170921/1758
Integer Underflow (Wrap or Wraparoun d)	08-Sep-21	10	Integer underflow can occur due to improper handling of incoming RTCP packets in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Voice & Music, Snapdragon Wearables CVE ID : CVE-2021-1920	https://www. qualcomm.co m/company/ product- security/bull etins/august- 2021-bulletin	H-QUA- WCN3- 170921/1759
Incorrect Type Conversion or Cast	08-Sep-21	4.6	Incorrect pointer argument passed to trusted application TA could result in un- intended memory operations in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Industrial IOT CVE ID : CVE-2021-1923	https://www. qualcomm.co m/company/ product- security/bull etins/august- 2021-bulletin	H-QUA- WCN3- 170921/1760
Exposure of Resource to Wrong Sphere	08-Sep-21	2.1	Lack of strict validation of bootmode can lead to information disclosure in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity,	https://www. qualcomm.co m/company/ product- security/bull etins/august-	H-QUA- WCN3- 170921/1761

1-2 2-3

0-1

5-6

6-7

7-8

8-9

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wearables	2021-bulletin	
			CVE ID : CVE-2021-1929		
Improper Restriction of Operations within the Bounds of a Memory Buffer	08-Sep-21	3.6	Possible out of bounds read due to incorrect validation of incoming buffer length in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile	https://www. qualcomm.co m/company/ product- security/bull etins/august- 2021-bulletin	H-QUA- WCN3- 170921/1762
			CVE ID : CVE-2021-1930		
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	08-Sep-21	10	Possible buffer overflow due to improper validation of device types during P2P search in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Woice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking CVE ID : CVE-2021-1972	https://www. qualcomm.co m/company/ product- security/bull etins/august- 2021-bulletin	H-QUA- WCN3- 170921/1763
wcn3950					
Exposure of Resource to Wrong Sphere	08-Sep-21	2.1	Child process can leak information from parent process due to numeric pids are getting compared and these pid can be reused in Snapdragon Auto, Snapdragon Compute,	https://www. qualcomm.co m/company/ product- security/bull etins/august- 2021-bulletin	H-QUA- WCN3- 170921/1764
CVSS Scoring Sc	ale 0-1	1-2	2-3 3-4 4-5 5-6 Page 615 of 1474	6-7 7-8	8-9 9-10

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables		
			CVE ID : CVE-2021-1904		
Loop with Unreachable Exit Condition ('Infinite Loop')	08-Sep-21	5	Loop with unreachable exit condition may occur due to improper handling of unsupported input in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Voice & Music, Snapdragon Wearables CVE ID : CVE-2021-1914	https://www. qualcomm.co m/company/ product- security/bull etins/august- 2021-bulletin	H-QUA- WCN3- 170921/1765
Out-of- bounds Write	08-Sep-21	10	Possible buffer underflow due to lack of check for negative indices values when processing user provided input in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Voice & Music, Snapdragon Wearables CVE ID : CVE-2021-1916	https://www. qualcomm.co m/company/ product- security/bull etins/august- 2021-bulletin	H-QUA- WCN3- 170921/1766
Integer Underflow (Wrap or Wraparoun d)	08-Sep-21	10	Integer underflow can occur when the RTCP length is lesser than than the actual blocks present in Snapdragon Auto, Snapdragon Compute,	https://www. qualcomm.co m/company/ product- security/bull	H-QUA- WCN3- 170921/1767
CVSS Scoring Sc	ale 0-1	1-2	2-3 3-4 4-5 5-6	6-7 7-8	8-9 9-10

Page 616 of 1474

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Voice & Music, Snapdragon Wearables	etins/august- 2021-bulletin	
			CVE ID : CVE-2021-1919		
Integer Underflow (Wrap or Wraparoun d)	08-Sep-21	10	Integer underflow can occur due to improper handling of incoming RTCP packets in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Voice & Music, Snapdragon Wearables	https://www. qualcomm.co m/company/ product- security/bull etins/august- 2021-bulletin	H-QUA- WCN3- 170921/1768
			CVE ID : CVE-2021-1920		
Incorrect Type Conversion or Cast	08-Sep-21	4.6	Incorrect pointer argument passed to trusted application TA could result in un- intended memory operations in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Industrial IOT CVE ID : CVE-2021-1923	https://www. qualcomm.co m/company/ product- security/bull etins/august- 2021-bulletin	H-QUA- WCN3- 170921/1769
Exposure of Resource to Wrong Sphere	08-Sep-21	2.1	Lack of strict validation of bootmode can lead to information disclosure in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wearables	https://www. qualcomm.co m/company/ product- security/bull etins/august- 2021-bulletin	H-QUA- WCN3- 170921/1770
CVSS Scoring Sc	ale 0-1	1-2	2-3 3-4 4-5 5-6	6-7 7-8	8-9 9-10

 3-4
 4-5

 Page 617 of 1474

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2021-1929		
Improper Restriction of Operations within the Bounds of a Memory Buffer	08-Sep-21	3.6	Possible out of bounds read due to incorrect validation of incoming buffer length in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile CVE ID : CVE-2021-1930	https://www. qualcomm.co m/company/ product- security/bull etins/august- 2021-bulletin	H-QUA- WCN3- 170921/1771
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	08-Sep-21	10	Possible buffer overflow due to improper validation of device types during P2P search in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Woice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking CVE ID : CVE-2021-1972	https://www. qualcomm.co m/company/ product- security/bull etins/august- 2021-bulletin	H-QUA- WCN3- 170921/1772
wcn3980	I			I	I
Exposure of Resource to Wrong Sphere	08-Sep-21	2.1	Child process can leak information from parent process due to numeric pids are getting compared and these pid can be reused in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile,	https://www. qualcomm.co m/company/ product- security/bull etins/august- 2021-bulletin	H-QUA- WCN3- 170921/1773

Γ		0.1	1.2	2.2	2.4		FC	C7	7.0	0.0	0.40
	CVSS Scoring Scale	0-1	1-2	2-3	3-4	4-5	5-6	6-7	/-8	8-9	9-10
				D	200 610 0	£1474					

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Snapdragon Voice & Music, Snapdragon Wearables		
			CVE ID : CVE-2021-1904		
Out-of- bounds Read	08-Sep-21	3.6	Buffer over read could occur due to incorrect check of buffer size while flashing emmc devices in Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking CVE ID : CVE-2021-1928	https://www. qualcomm.co m/company/ product- security/bull etins/august- 2021-bulletin	H-QUA- WCN3- 170921/1774
Exposure of Resource to Wrong Sphere	08-Sep-21	2.1	Lack of strict validation of bootmode can lead to information disclosure in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wearables CVE ID : CVE-2021-1929	https://www. qualcomm.co m/company/ product- security/bull etins/august- 2021-bulletin	H-QUA- WCN3- 170921/1775
Improper Restriction of Operations within the Bounds of a Memory Buffer	08-Sep-21	3.6	Possible out of bounds read due to incorrect validation of incoming buffer length in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile CVE ID : CVE-2021-1930	https://www. qualcomm.co m/company/ product- security/bull etins/august- 2021-bulletin	H-QUA- WCN3- 170921/1776

CVSS Scoring Scale	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10
			P	age 619 c	of 1474					

Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
08-Sep-21	10	Possible buffer overflow due to improper validation of device types during P2P search in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Woice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking CVE ID : CVE-2021-1972	https://www. qualcomm.co m/company/ product- security/bull etins/august- 2021-bulletin	H-QUA- WCN3- 170921/1777
08-Sep-21	2.1	Child process can leak information from parent process due to numeric pids are getting compared and these pid can be reused in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables CVE ID : CVE-2021-1904	https://www. qualcomm.co m/company/ product- security/bull etins/august- 2021-bulletin	H-QUA- WCN3- 170921/1778
08-Sep-21	5	Loop with unreachable exit condition may occur due to improper handling of unsupported input in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT,	https://www. qualcomm.co m/company/ product- security/bull etins/august- 2021-bulletin	H-QUA- WCN3- 170921/1779
	08-Sep-21	08-Sep-21 10 08-Sep-21 2.1 08-Sep-21 5.1	08-Sep-21Image: Construction of the section of the secti	08-Sep-21Image: Construction of device types during P2P search in Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Nobile, Snapdragon Nobile, Snapdragon Nobile, Snapdragon Wired Infrastructure and Networkinghttps://www. qualcomm.co m/company/ product- security/bull etins/august- 2021-bulletin08-Sep-212.1Child process can leak information from parent process due to numeric pids are getting compared and these pid can be reused in Snapdragon Nobile, Snapdragon Consumer IOT, Snapdragon Consumer IOT, Snapdragon Muto, Snapdragon Nobile, Snapdragon Nobile, Snapdrago

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Snapdragon IoT, Snapdragon Voice & Music, Snapdragon Wearables		
			CVE ID : CVE-2021-1914		
Out-of- bounds Write	08-Sep-21	10	Possible buffer underflow due to lack of check for negative indices values when processing user provided input in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Voice & Music, Snapdragon Wearables	https://www. qualcomm.co m/company/ product- security/bull etins/august- 2021-bulletin	H-QUA- WCN3- 170921/1780
			CVE ID : CVE-2021-1916		
Integer Underflow (Wrap or Wraparoun d)	08-Sep-21	10	Integer underflow can occur when the RTCP length is lesser than than the actual blocks present in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Voice & Music, Snapdragon Wearables	https://www. qualcomm.co m/company/ product- security/bull etins/august- 2021-bulletin	H-QUA- WCN3- 170921/1781
			CVE ID : CVE-2021-1919		
Integer Underflow (Wrap or Wraparoun d)	08-Sep-21	10	Integer underflow can occur due to improper handling of incoming RTCP packets in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon	https://www. qualcomm.co m/company/ product- security/bull etins/august- 2021-bulletin	H-QUA- WCN3- 170921/1782

1-2

0-1

4-5

6-7

5-6

7-8

8-9

9-10

3-4

		Voice & Music, Snapdragon		
		Wearables		
		CVE ID : CVE-2021-1920		
08-Sep-21	4.6	Incorrect pointer argument passed to trusted application TA could result in un- intended memory operations in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Industrial IOT CVE ID : CVE-2021-1923	https://www. qualcomm.co m/company/ product- security/bull etins/august- 2021-bulletin	H-QUA- WCN3- 170921/1783
08-Sep-21	2.1	Lack of strict validation of bootmode can lead to information disclosure in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wearables CVE ID : CVE-2021-1929	https://www. qualcomm.co m/company/ product- security/bull etins/august- 2021-bulletin	H-QUA- WCN3- 170921/1784
08-Sep-21	3.6	Possible out of bounds read due to incorrect validation of incoming buffer length in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile CVE ID : CVE-2021-1930	https://www. qualcomm.co m/company/ product- security/bull etins/august- 2021-bulletin	H-QUA- WCN3- 170921/1785
08-Sep-21	10	Possible buffer overflow due to improper validation of device types during P2P search in Snapdragon Auto, Snapdragon Compute,	https://www. qualcomm.co m/company/ product- security/bull	H-QUA- WCN3- 170921/1786
	08-Sep-21 08-Sep-21	1 1 08-Sep-21 2.1 08-Sep-21 3.6 08-Sep-21 10	08-Sep-214.6passed to trusted application TA could result in un- intended memory operations Snapdragon Auto, Snapdragon Compute, Snapdragon Industrial IOT CVE ID : CVE-2021-1923 08-Sep-218 4.6Lack of strict validation of bootmode can lead to information disclosure in Snapdragon Compute, Snapdragon Compute, Snapdragon Compute, Snapdragon Compute, Snapdragon Compute, Snapdragon Compute, Snapdragon Consumer IOT, Snapdragon Consumer IOT, Snapdragon Mobile, Snapdragon Compute, Snapdragon Compute, Snapdragon Mobile Snapdragon Mobile Snapdragon Mobile Snapdragon Mobile Snapdragon Mobile08-Sep-2110Possible buffer overflow due to improper validation of device types during P2P search in Snapdragon Auto, Snapdragon Auto, Snapdragon Mobile	08-Sep-21A.6passed to trusted application TA could result in un- intended memory operations in Snapdragon Auto, Snapdragon Compute, Snapdragon Industrial IOT CVE ID : CVE-2021-1923https://www. qualcomm.co m/company/ product- security/bull etins/august- 2021-bulletin08-Sep-212.1Lack of strict validation of bootmode can lead to information disclosure in Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Consumer IOT, Snapdragon Consumer IOT, Snapdragon Consumer IOT, Snapdragon Mobile, Snapdragon Mobile, Snapdragon Mobile, Snapdragon Mobile, Snapdragon Consumer IOT,

Page 622 of 1474

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID		
Buffer Overflow')			Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking CVE ID : CVE-2021-1972	etins/august- 2021-bulletin			
wcn3990				<u> </u>			
Exposure of Resource to Wrong Sphere	08-Sep-21	2.1	Child process can leak information from parent process due to numeric pids are getting compared and these pid can be reused in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables CVE ID : CVE-2021-1904	https://www. qualcomm.co m/company/ product- security/bull etins/august- 2021-bulletin	H-QUA- WCN3- 170921/1787		
Exposure of Resource to Wrong Sphere	08-Sep-21	2.1	Lack of strict validation of bootmode can lead to information disclosure in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wearables CVE ID : CVE-2021-1929	https://www. qualcomm.co m/company/ product- security/bull etins/august- 2021-bulletin	H-QUA- WCN3- 170921/1788		
Improper	08-Sep-21	3.6	Possible out of bounds read	https://www.	H-QUA-		
RestrictionImage: due to incorrect validation of pullcomm.coWCN3-CVSS Scoring Scale0-11-22-33-44-55-66-77-88-99-10							

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
of Operations within the Bounds of a Memory Buffer			incoming buffer length in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile CVE ID : CVE-2021-1930	m/company/ product- security/bull etins/august- 2021-bulletin	170921/1789
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	08-Sep-21	10	Possible buffer overflow due to improper validation of device types during P2P search in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Woice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking CVE ID : CVE-2021-1972	https://www. qualcomm.co m/company/ product- security/bull etins/august- 2021-bulletin	H-QUA- WCN3- 170921/1790
wcn3991					
Exposure of Resource to Wrong Sphere	08-Sep-21	2.1	Child process can leak information from parent process due to numeric pids are getting compared and these pid can be reused in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wearables CVE ID : CVE-2021-1904	https://www. qualcomm.co m/company/ product- security/bull etins/august- 2021-bulletin	H-QUA- WCN3- 170921/1791
CVSS Scoring Sca	ale 0-1	1-2	2-3 3-4 4-5 5-6	6-7 7-8	8-9 9-10

Page 624 of 1474

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Loop with Unreachable Exit Condition ('Infinite Loop')	08-Sep-21	5	Loop with unreachable exit condition may occur due to improper handling of unsupported input in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Voice & Music, Snapdragon Wearables CVE ID : CVE-2021-1914	https://www. qualcomm.co m/company/ product- security/bull etins/august- 2021-bulletin	H-QUA- WCN3- 170921/1792
Out-of- bounds Write	08-Sep-21	10	Possible buffer underflow due to lack of check for negative indices values when processing user provided input in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Voice & Music, Snapdragon Wearables CVE ID : CVE-2021-1916	https://www. qualcomm.co m/company/ product- security/bull etins/august- 2021-bulletin	H-QUA- WCN3- 170921/1793
Integer Underflow (Wrap or Wraparoun d)	08-Sep-21	10	Integer underflow can occur when the RTCP length is lesser than than the actual blocks present in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Voice & Music, Snapdragon Wearables CVE ID : CVE-2021-1919	https://www. qualcomm.co m/company/ product- security/bull etins/august- 2021-bulletin	H-QUA- WCN3- 170921/1794

CVSS Scoring Scale	0-1	1-2	2-3	3-4	4-5	5-6	6-7
			-		c – .		

7-8

8-9

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Integer Underflow (Wrap or Wraparoun d)	08-Sep-21	10	Integer underflow can occur due to improper handling of incoming RTCP packets in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Voice & Music, Snapdragon Wearables CVE ID : CVE-2021-1920	https://www. qualcomm.co m/company/ product- security/bull etins/august- 2021-bulletin	H-QUA- WCN3- 170921/1795
Incorrect Type Conversion or Cast	08-Sep-21	4.6	Incorrect pointer argument passed to trusted application TA could result in un- intended memory operations in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Industrial IOT CVE ID : CVE-2021-1923	https://www. qualcomm.co m/company/ product- security/bull etins/august- 2021-bulletin	H-QUA- WCN3- 170921/1796
Exposure of Resource to Wrong Sphere	08-Sep-21	2.1	Lack of strict validation of bootmode can lead to information disclosure in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wearables CVE ID : CVE-2021-1929	https://www. qualcomm.co m/company/ product- security/bull etins/august- 2021-bulletin	H-QUA- WCN3- 170921/1797
Improper Restriction of Operations within the Bounds of a	08-Sep-21	3.6	Possible out of bounds read due to incorrect validation of incoming buffer length in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity,	https://www. qualcomm.co m/company/ product- security/bull etins/august-	H-QUA- WCN3- 170921/1798

0-1

4-5

6-7

5-6

7-8

8-9

9-10

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Memory Buffer			Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile	2021-bulletin	
			CVE ID : CVE-2021-1930		
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	08-Sep-21	10	Possible buffer overflow due to improper validation of device types during P2P search in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Woice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking CVE ID : CVE-2021-1972	https://www. qualcomm.co m/company/ product- security/bull etins/august- 2021-bulletin	H-QUA- WCN3- 170921/1799
wcn3998					
Exposure of Resource to Wrong Sphere	08-Sep-21	2.1	Child process can leak information from parent process due to numeric pids are getting compared and these pid can be reused in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wearables CVE ID : CVE-2021-1904	https://www. qualcomm.co m/company/ product- security/bull etins/august- 2021-bulletin	H-QUA- WCN3- 170921/1800
Loop with Unreachable Exit Condition	08-Sep-21	5	Loop with unreachable exit condition may occur due to improper handling of unsupported input in	https://www. qualcomm.co m/company/ product-	H-QUA- WCN3- 170921/1801
CVSS Scoring Sc	ale 0-1	1-2	2-3 3-4 4-5 5-6	6-7 7-8	8-9 9-10

Page 627 of 1474

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
('Infinite Loop')			Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Voice & Music, Snapdragon Wearables	security/bull etins/august- 2021-bulletin	
Out-of- bounds Write	08-Sep-21	10	CVE ID : CVE-2021-1914 Possible buffer underflow due to lack of check for negative indices values when processing user provided input in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Voice & Music, Snapdragon Wearables CVE ID : CVE-2021-1916	https://www. qualcomm.co m/company/ product- security/bull etins/august- 2021-bulletin	H-QUA- WCN3- 170921/1802
Integer Underflow (Wrap or Wraparoun d)	08-Sep-21	10	Integer underflow can occur when the RTCP length is lesser than than the actual blocks present in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Voice & Music, Snapdragon Wearables CVE ID : CVE-2021-1919	https://www. qualcomm.co m/company/ product- security/bull etins/august- 2021-bulletin	H-QUA- WCN3- 170921/1803
Integer Underflow (Wrap or Wraparoun	08-Sep-21	10	Integer underflow can occur due to improper handling of incoming RTCP packets in Snapdragon Auto,	https://www. qualcomm.co m/company/ product-	H-QUA- WCN3- 170921/1804

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

or CastSnapdragon Connectivity, Snapdragon Industrial IOTetins/august- 2021-bulletinExposure of Resource to Wrong Sphere08-Sep-21Lack of strict validation of bootmode can lead to information disclosure in Snapdragon Compute, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Wearableshttps://www. qualcomm.co m/company/ product- security/bull etins/august- 2021-bulletinH-QUA- WCN3- 170921/180/ H-QUA- WCN3- 170921/180/ etins/august- 2021-bulletinImproper Restriction of Operations within the Bounds of a Memory08-Sep-21APossible out of bounds read due to incorrect validation of incoming buffer length in Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Connectivity, Snapdragon Connectivity, Snapdragon Connectivity, Snapdragon Connectivity, Snapdragon Connectivity, Snapdragon Connectivity, Snapdragon Industrial IOT, ZO21-bulletinH-QUA- WCN3- I70921/180/ WCN3- I70921/180/	Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Incorrect Type Conversion or Cast08-Sep-21assed to trusted application TA could result in un- intended memory operations in Snapdragon Auto, Snapdragon Compute, Snapdragon Compute, Snapdragon Industrial IOThttps://www. qualcomm.co m/company/ product- security/bull etins/august- 2021-bulletinH-QUA- WCN3- 170921/180Exposure of Resource to Wrong Sphere08-Sep-212.1Lack of strict validation of bootmode can lead to information disclosure in Snapdragon Compute, Snapdragon Compute, Snapdragon Compute, Snapdragon Compute, Snapdragon Compute, Snapdragon Compute, Snapdragon Muto, Snapdragon Consumer IOT, Snapdragon Mobile, Snapdragon Mobile, Snapdragon Mobile, Snapdragon Mobile, Snapdragon Mobile, Snapdragon Mobile, Snapdragon Muto, Snapdragon Mobile, Snapdragon Muto, Snapdragon Muto, Snapdragon Muto, Snapdragon Muto, Snapdragon Mobile, Snapdragon Mobile, Snapdragon Muto, Snapdragon Muto, Snapdragon Muto, Snapdragon Muto, Snapdragon Muto, Snapdragon Muto, Snapdragon Compute, Snapdragon Muto, Snapdragon Compute, Snapdragon Muto, Snapdragon Muto, Snapdragon Compute, Snapdragon Compute, Snapdragon Compute, Snapdragon Compute, Snapdragon Compute, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Industrial IOT, etins/august- 2021-bulletinH-QUA- WCN3- H-QUA- WCN3- H-QUA- WCN3- H-QUA- WCN3- H-QUA- WCN3- H-QUA-<	d)			Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Voice & Music, Snapdragon Wearables	etins/august-	
Exposure of Resource to Wrong Sphere08-Sep-212.1bootmode can lead to information disclosure in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wearableshttps://www. qualcomm.co m/company/ product- security/bull 	Type Conversion	08-Sep-21	4.6	passed to trusted application TA could result in un- intended memory operations in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Industrial IOT	qualcomm.co m/company/ product- security/bull etins/august-	-
Improper Restriction of Operations within the Bounds of a Memory08-Sep-21due to incorrect validation of incoming buffer length in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT,https://www. qualcomm.co m/company/ product- to 170921/1807	Resource to Wrong	08-Sep-21	2.1	bootmode can lead to information disclosure in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wearables	qualcomm.co m/company/ product- security/bull etins/august-	-
CVE ID : CVE-2021-1930	Restriction of Operations within the Bounds of a	08-Sep-21	3.6	due to incorrect validation of incoming buffer length in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile	qualcomm.co m/company/ product- security/bull etins/august-	-

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	08-Sep-21	10	Possible buffer overflow due to improper validation of device types during P2P search in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Woice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking CVE ID : CVE-2021-1972	https://www. qualcomm.co m/company/ product- security/bull etins/august- 2021-bulletin	H-QUA- WCN3- 170921/1808
wcn3999					
Exposure of Resource to Wrong Sphere	08-Sep-21	2.1	Child process can leak information from parent process due to numeric pids are getting compared and these pid can be reused in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables CVE ID : CVE-2021-1904	https://www. qualcomm.co m/company/ product- security/bull etins/august- 2021-bulletin	H-QUA- WCN3- 170921/1809
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	08-Sep-21	10	Possible buffer overflow due to improper validation of device types during P2P search in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile,	https://www. qualcomm.co m/company/ product- security/bull etins/august- 2021-bulletin	H-QUA- WCN3- 170921/1810

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking CVE ID : CVE-2021-1972		
wcn6740					
Exposure of Resource to Wrong Sphere	08-Sep-21	2.1	Child process can leak information from parent process due to numeric pids are getting compared and these pid can be reused in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wearables CVE ID : CVE-2021-1904	https://www. qualcomm.co m/company/ product- security/bull etins/august- 2021-bulletin	H-QUA- WCN6- 170921/1811
Out-of- bounds Write	08-Sep-21	10	Possible buffer underflow due to lack of check for negative indices values when processing user provided input in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Voice & Music, Snapdragon Wearables CVE ID : CVE-2021-1916	https://www. qualcomm.co m/company/ product- security/bull etins/august- 2021-bulletin	H-QUA- WCN6- 170921/1812
Incorrect Type Conversion or Cast	08-Sep-21	4.6	Incorrect pointer argument passed to trusted application TA could result in un- intended memory operations	https://www. qualcomm.co m/company/ product-	H-QUA- WCN6- 170921/1813
CVSS Scoring Sco	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
			in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Industrial IOT CVE ID : CVE-2021-1923	security/bull etins/august- 2021-bulletin	
Exposure of Resource to Wrong Sphere	08-Sep-21	2.1	Lack of strict validation of bootmode can lead to information disclosure in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wearables CVE ID : CVE-2021-1929	https://www. qualcomm.co m/company/ product- security/bull etins/august- 2021-bulletin	H-QUA- WCN6- 170921/1814
Improper Restriction of Operations within the Bounds of a Memory Buffer	08-Sep-21	3.6	Possible out of bounds read due to incorrect validation of incoming buffer length in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile CVE ID : CVE-2021-1930	https://www. qualcomm.co m/company/ product- security/bull etins/august- 2021-bulletin	H-QUA- WCN6- 170921/1815
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	08-Sep-21	10	Possible buffer overflow due to improper validation of device types during P2P search in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Woice & Music, Snapdragon Wearables, Snapdragon Wired	https://www. qualcomm.co m/company/ product- security/bull etins/august- 2021-bulletin	H-QUA- WCN6- 170921/1816

0-1

1-2

6-7

5-6

7-8

8-9

			Infrastructure and Networking		
			CVE ID : CVE-2021-1972		
			CVE ID : CVE-2021-1972		
wcn6750				F	Г
Exposure of Resource to Wrong Sphere	08-Sep-21	2.1	Child process can leak information from parent process due to numeric pids are getting compared and these pid can be reused in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wearables CVE ID : CVE-2021-1904	https://www. qualcomm.co m/company/ product- security/bull etins/august- 2021-bulletin	H-QUA- WCN6- 170921/1817
Loop with Unreachable Exit Condition ('Infinite Loop')	08-Sep-21	5	Loop with unreachable exit condition may occur due to improper handling of unsupported input in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Voice & Music, Snapdragon Wearables CVE ID : CVE-2021-1914	https://www. qualcomm.co m/company/ product- security/bull etins/august- 2021-bulletin	H-QUA- WCN6- 170921/1818
Out-of- bounds Write	08-Sep-21	10	Possible buffer underflow due to lack of check for negative indices values when processing user provided input in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity,	https://www. qualcomm.co m/company/ product- security/bull etins/august- 2021-bulletin	H-QUA- WCN6- 170921/1819

		Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Voice & Music, Snapdragon Wearables CVE ID : CVE-2021-1916		
		Integer underflow can occur		
8-Sep-21	10	when the RTCP length is lesser than than the actual blocks present in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Voice & Music, Snapdragon Wearables	https://www. qualcomm.co m/company/ product- security/bull etins/august- 2021-bulletin	H-QUA- WCN6- 170921/1820
		CVE ID : CVE-2021-1919		
8-Sep-21	10	Integer underflow can occur due to improper handling of incoming RTCP packets in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Voice & Music, Snapdragon Wearables	https://www. qualcomm.co m/company/ product- security/bull etins/august- 2021-bulletin	H-QUA- WCN6- 170921/1821
		CVE ID : CVE-2021-1920		
8-Sep-21	4.6	Incorrect pointer argument passed to trusted application TA could result in un- intended memory operations in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Industrial IOT	https://www. qualcomm.co m/company/ product- security/bull etins/august- 2021-bulletin	H-QUA- WCN6- 170921/1822
8	-Sep-21	-Sep-21 10	-Sep-2110Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Industrial IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Voice & Music, Snapdragon Wearables-Sep-2110Integer underflow can occur due to improper handling of incoming RTCP packets in Snapdragon Compute, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Compute, Snapdragon Industrial IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Voice & Music, Snapdragon Snapdragon Connectivity, Snapdragon Connectivity, Snapdragon Connectivity, Snapdragon Connectivity, Snapdragon Industrial IOT	-Sep-21Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Industrial IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Voice & Music, Snapdragon Wearablesqualcomm.co m/company/ product- security/bull etins/august- 2021-bulletin-Sep-2110Integer underflow can occur due to improper handling of incoming RTCP packets in Snapdragon Compute, Snapdragon Connectivity, Snapdragon Connectivity, Snapdragon Connectivity, Snapdragon Industrial IOT, Snapdragon Industrial IOT, Snapdragon Industrial IOT, Snapdragon Industrial IOT,

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2021-1923		
Exposure of Resource to Wrong Sphere	08-Sep-21	2.1	Lack of strict validation of bootmode can lead to information disclosure in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wearables CVE ID : CVE-2021-1929	https://www. qualcomm.co m/company/ product- security/bull etins/august- 2021-bulletin	H-QUA- WCN6- 170921/1823
			Possible out of bounds read		
Improper Restriction of Operations within the Bounds of a Memory Buffer	08-Sep-21	3.6	due to incorrect validation of incoming buffer length in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile CVE ID : CVE-2021-1930	https://www. qualcomm.co m/company/ product- security/bull etins/august- 2021-bulletin	H-QUA- WCN6- 170921/1824
			Possible buffer overflow due		
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	08-Sep-21	10	Possible buffer overflow due to improper validation of device types during P2P search in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Woice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking CVE ID : CVE-2021-1972	https://www. qualcomm.co m/company/ product- security/bull etins/august- 2021-bulletin	H-QUA- WCN6- 170921/1825
wcn6850					
CVSS Scoring Sc	ale 0-1	1-2	2-3 3-4 4-5 5-6	6-7 7-8	8-9 9-10
			Page 635 of 1474		

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Exposure of Resource to Wrong Sphere	08-Sep-21	2.1	Child process can leak information from parent process due to numeric pids are getting compared and these pid can be reused in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wearables CVE ID : CVE-2021-1904	https://www. qualcomm.co m/company/ product- security/bull etins/august- 2021-bulletin	H-QUA- WCN6- 170921/1826
Loop with Unreachable Exit Condition ('Infinite Loop')	08-Sep-21	5	Loop with unreachable exit condition may occur due to improper handling of unsupported input in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Voice & Music, Snapdragon Wearables CVE ID : CVE-2021-1914	https://www. qualcomm.co m/company/ product- security/bull etins/august- 2021-bulletin	H-QUA- WCN6- 170921/1827
Out-of- bounds Write	08-Sep-21	10	Possible buffer underflow due to lack of check for negative indices values when processing user provided input in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Voice & Music, Snapdragon Wearables	https://www. qualcomm.co m/company/ product- security/bull etins/august- 2021-bulletin	H-QUA- WCN6- 170921/1828
CVSS Scoring Sc	ale 0-1	1-2	2-3 3-4 4-5 5-6	6-7 7-8	8-9 9-10

Page 636 of 1474

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2021-1916		
Integer Underflow (Wrap or Wraparoun d)	08-Sep-21	10	Integer underflow can occur when the RTCP length is lesser than than the actual blocks present in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Voice & Music, Snapdragon Wearables CVE ID : CVE-2021-1919	https://www. qualcomm.co m/company/ product- security/bull etins/august- 2021-bulletin	H-QUA- WCN6- 170921/1829
Integer Underflow (Wrap or Wraparoun d)	08-Sep-21	10	Integer underflow can occur due to improper handling of incoming RTCP packets in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Voice & Music, Snapdragon Wearables CVE ID : CVE-2021-1920	https://www. qualcomm.co m/company/ product- security/bull etins/august- 2021-bulletin	H-QUA- WCN6- 170921/1830
Incorrect Type Conversion or Cast	08-Sep-21	4.6	Incorrect pointer argument passed to trusted application TA could result in un- intended memory operations in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Industrial IOT CVE ID : CVE-2021-1923	https://www. qualcomm.co m/company/ product- security/bull etins/august- 2021-bulletin	H-QUA- WCN6- 170921/1831
Exposure of Resource to Wrong Sphere CVSS Scoring Sc	08-Sep-21 ale 0-1	2.1	Lack of strict validation of bootmode can lead to information disclosure in Snapdragon Auto, 2-3 3-4 4-5 5-6	https://www. qualcomm.co m/company/ product-	H-QUA- WCN6- 170921/1832 8-9 9-10

Page 637 of 1474

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wearables CVE ID : CVE-2021-1929	security/bull etins/august- 2021-bulletin	
Improper Restriction of Operations within the Bounds of a Memory Buffer	08-Sep-21	3.6	Possible out of bounds read due to incorrect validation of incoming buffer length in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile CVE ID : CVE-2021-1930	https://www. qualcomm.co m/company/ product- security/bull etins/august- 2021-bulletin	H-QUA- WCN6- 170921/1833
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	08-Sep-21	10	Possible buffer overflow due to improper validation of device types during P2P search in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Woice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking CVE ID : CVE-2021-1972	https://www. qualcomm.co m/company/ product- security/bull etins/august- 2021-bulletin	H-QUA- WCN6- 170921/1834
wcn6851				-	
Exposure of Resource to Wrong Sphere	08-Sep-21	2.1	Child process can leak information from parent process due to numeric pids are getting compared and these pid can be reused in	https://www. qualcomm.co m/company/ product- security/bull	H-QUA- WCN6- 170921/1835
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 Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables CVE ID : CVE-2021-1904	etins/august- 2021-bulletin	
Loop with Unreachable Exit Condition ('Infinite Loop')	08-Sep-21	5	Loop with unreachable exit condition may occur due to improper handling of unsupported input in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Voice & Music, Snapdragon Wearables CVE ID : CVE-2021-1914	https://www. qualcomm.co m/company/ product- security/bull etins/august- 2021-bulletin	H-QUA- WCN6- 170921/1836
Out-of- bounds Write	08-Sep-21	10	Possible buffer underflow due to lack of check for negative indices values when processing user provided input in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Voice & Music, Snapdragon Wearables CVE ID : CVE-2021-1916	https://www. qualcomm.co m/company/ product- security/bull etins/august- 2021-bulletin	H-QUA- WCN6- 170921/1837
Integer Underflow (Wrap or	08-Sep-21	10	Integer underflow can occur when the RTCP length is lesser than than the actual	https://www. qualcomm.co m/company/	H-QUA- WCN6- 170921/1838

Page 639 of 1474

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Wraparoun d)			blocks present in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Voice & Music, Snapdragon Wearables CVE ID : CVE-2021-1919	product- security/bull etins/august- 2021-bulletin	
Integer Underflow (Wrap or Wraparoun d)	08-Sep-21	10	Integer underflow can occur due to improper handling of incoming RTCP packets in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Voice & Music, Snapdragon Wearables CVE ID : CVE-2021-1920	https://www. qualcomm.co m/company/ product- security/bull etins/august- 2021-bulletin	H-QUA- WCN6- 170921/1839
Incorrect Type Conversion or Cast	08-Sep-21	4.6	Incorrect pointer argument passed to trusted application TA could result in un- intended memory operations in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Industrial IOT CVE ID : CVE-2021-1923	https://www. qualcomm.co m/company/ product- security/bull etins/august- 2021-bulletin	H-QUA- WCN6- 170921/1840
Exposure of Resource to Wrong Sphere	08-Sep-21	2.1	Lack of strict validation of bootmode can lead to information disclosure in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT,	https://www. qualcomm.co m/company/ product- security/bull etins/august- 2021-bulletin	H-QUA- WCN6- 170921/1841

1-2 2-3

0-1

5-6

6-7

7-8

8-9

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Snapdragon Mobile, Snapdragon Wearables CVE ID : CVE-2021-1929		
Improper Restriction of Operations within the Bounds of a Memory Buffer	08-Sep-21	3.6	Possible out of bounds read due to incorrect validation of incoming buffer length in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile CVE ID : CVE-2021-1930	https://www. qualcomm.co m/company/ product- security/bull etins/august- 2021-bulletin	H-QUA- WCN6- 170921/1842
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	08-Sep-21	10	Possible buffer overflow due to improper validation of device types during P2P search in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Woice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking CVE ID : CVE-2021-1972	https://www. qualcomm.co m/company/ product- security/bull etins/august- 2021-bulletin	H-QUA- WCN6- 170921/1843
wcn6855				I	I
Exposure of Resource to Wrong Sphere	08-Sep-21	2.1	Child process can leak information from parent process due to numeric pids are getting compared and these pid can be reused in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT,	https://www. qualcomm.co m/company/ product- security/bull etins/august- 2021-bulletin	H-QUA- WCN6- 170921/1844
CVSS Scoring Sc	ale 0-1	1-2	2-3 3-4 4-5 5-6	6-7 7-8	8-9 9-10

			Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables		
			CVE ID : CVE-2021-1904		
Loop with Unreachable Exit Condition ('Infinite Loop')	08-Sep-21	5	Loop with unreachable exit condition may occur due to improper handling of unsupported input in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Voice & Music, Snapdragon Wearables	https://www. qualcomm.co m/company/ product- security/bull etins/august- 2021-bulletin	H-QUA- WCN6- 170921/1845
			CVE ID : CVE-2021-1914		
Out-of- bounds Write	08-Sep-21	10	Possible buffer underflow due to lack of check for negative indices values when processing user provided input in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Voice & Music, Snapdragon Wearables CVE ID : CVE-2021-1916	https://www. qualcomm.co m/company/ product- security/bull etins/august- 2021-bulletin	H-QUA- WCN6- 170921/1846
Integer Underflow (Wrap or Wraparoun d)	08-Sep-21	10	Integer underflow can occur when the RTCP length is lesser than than the actual blocks present in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT,	https://www. qualcomm.co m/company/ product- security/bull etins/august- 2021-bulletin	H-QUA- WCN6- 170921/1847
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 Industrial IOT, Snapdragon IoT, Snapdragon Voice & Music, Snapdragon Wearables		
			CVE ID : CVE-2021-1919		
Integer Underflow (Wrap or Wraparoun d)	08-Sep-21	10	Integer underflow can occur due to improper handling of incoming RTCP packets in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Voice & Music, Snapdragon Wearables	https://www. qualcomm.co m/company/ product- security/bull etins/august- 2021-bulletin	H-QUA- WCN6- 170921/1848
			CVE ID : CVE-2021-1920		
Incorrect Type Conversion or Cast	08-Sep-21	4.6	Incorrect pointer argument passed to trusted application TA could result in un- intended memory operations in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Industrial IOT CVE ID : CVE-2021-1923	https://www. qualcomm.co m/company/ product- security/bull etins/august- 2021-bulletin	H-QUA- WCN6- 170921/1849
Improper Restriction of Operations within the Bounds of a Memory Buffer	08-Sep-21	3.6	Possible out of bounds read due to incorrect validation of incoming buffer length in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile CVE ID : CVE-2021-1930	https://www. qualcomm.co m/company/ product- security/bull etins/august- 2021-bulletin	H-QUA- WCN6- 170921/1850
wcn6856					

0-1

1-2

7-8

5-6

6-7

8-9

Exposure of Resource to Wrong Sphere08-Sep-212.1Child process can leak information from parent process due to numeric pids are getting compared and these pid can be reused in Snapdragon Conneutivity, Snapdragon Consumer 107, Snapdragon Industrial 107, Snapdragon Nuto, Snapdragon Ocnsumer 107, Snapdragon Ocnsumer 107, Snapdragon Nuto, Snapdragon Ocneutivity, Snapdragon Ocnsumer 107, Snapdragon Ocnsumer 107, Snapdragon Noble, Snapdragon Ocnsumer 107, Snapdragon Ocnsumer 107, Snapdragon Ocneutivity, Snapdragon Ocneutivity, Snapdragon Ocneutivity, Snapdragon Ocneutivity, Snapdragon Ocneutivity, Snapdragon Ocneutivity, Snapdragon Ocneutivity, Snapdragon Ocneutivity, Snapdragon Comsumer 107, Snapdragon Comsumer 107, Snapdragon Consumer 107, <th>Weakness</th> <th>Publish Date</th> <th>CVSS</th> <th>Description & CVE ID</th> <th>Patch</th> <th>NCIIPC ID</th>	Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Loop with Unreachable Exit Condition 	Resource to Wrong	08-Sep-21	2.1	information from parent process due to numeric pids are getting compared and these pid can be reused in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wearables	qualcomm.co m/company/ product- security/bull etins/august-	WCN6-
Out-of- bounds08-Sep-2110due to lack of check for negative indices values when processing user provided input in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragonhttps://www. qualcomm.co m/company/H-QUA- WCN6- 170921/1853 etins/august- 2021-bulletin	Unreachable Exit Condition ('Infinite	08-Sep-21	5	condition may occur due to improper handling of unsupported input in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Voice & Music, Snapdragon Wearables	qualcomm.co m/company/ product- security/bull etins/august-	WCN6-
	bounds	08-Sep-21	10	due to lack of check for negative indices values when processing user provided input in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Voice & Music, Snapdragon	qualcomm.co m/company/ product- security/bull etins/august-	WCN6-

Page 644 of 1474

Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
		CVE ID : CVE-2021-1916		
08-Sep-21	10	Integer underflow can occur when the RTCP length is lesser than than the actual blocks present in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Voice & Music, Snapdragon Wearables CVE ID : CVE-2021-1919	https://www. qualcomm.co m/company/ product- security/bull etins/august- 2021-bulletin	H-QUA- WCN6- 170921/1854
08-Sep-21	10	Integer underflow can occur due to improper handling of incoming RTCP packets in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Voice & Music, Snapdragon Wearables CVE ID : CVE-2021-1920	https://www. qualcomm.co m/company/ product- security/bull etins/august- 2021-bulletin	H-QUA- WCN6- 170921/1855
08-Sep-21	4.6	Incorrect pointer argument passed to trusted application TA could result in un- intended memory operations in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Industrial IOT CVE ID : CVE-2021-1923	https://www. qualcomm.co m/company/ product- security/bull etins/august- 2021-bulletin	H-QUA- WCN6- 170921/1856
08-Sep-21	2.1	Lack of strict validation of bootmode can lead to information disclosure in Snapdragon Auto,	https://www. qualcomm.co m/company/ product-	H-QUA- WCN6- 170921/1857 8-9 9-10
	08-Sep-21 08-Sep-21	Image: marrier of the second secon	Image: construct of the second seco	O8-Sep-21IOCVE ID: CVE-2021-1916Integer underflow can occur lnteger underflow can occur lesser than than the actual blocks present in Snapdragon Auto, Snapdragon Compute, Snapdragon Industrial IOT, Snapdragon Industrial IOT, Snapdragon Industrial IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Wearableshttps://www. qualcomm.co m/company/ product- security/bull etins/august- 2021-bulletin08-Sep-2110Integer underflow can occur Nearableshttps://www. qualcomm.co m/company/ product- security/bull etins/august- 2021-bulletin08-Sep-2110Integer underflow can occur snapdragon Industrial IOT, Snapdragon Consumer IOT, Snapdragon Compute, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Compute, Snapdragon Compute, Snapdragon Compute, Snapdragon Compute, Snapdragon Industrial IOT, Snapdragon Industrial IOT Napardagon Industr

Page 645 of 1474

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wearables CVE ID : CVE-2021-1929	security/bull etins/august- 2021-bulletin	
Improper Restriction of Operations within the Bounds of a Memory Buffer	08-Sep-21	3.6	Possible out of bounds read due to incorrect validation of incoming buffer length in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile CVE ID : CVE-2021-1930	https://www. qualcomm.co m/company/ product- security/bull etins/august- 2021-bulletin	H-QUA- WCN6- 170921/1858
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	08-Sep-21	10	Possible buffer overflow due to improper validation of device types during P2P search in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Woice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking CVE ID : CVE-2021-1972	https://www. qualcomm.co m/company/ product- security/bull etins/august- 2021-bulletin	H-QUA- WCN6- 170921/1859
whs9410					
Loop with Unreachable Exit Condition ('Infinite	08-Sep-21	5	Loop with unreachable exit condition may occur due to improper handling of unsupported input in Snapdragon Auto,	https://www. qualcomm.co m/company/ product- security/bull	H-QUA- WHS9- 170921/1860
CVSS Scoring Scale 0-1 1-2 2-3 3-4 4-5 5-6 6-7 7-8 8-9 9-10 Page 646 of 1474					

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Loop')			Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Voice & Music, Snapdragon Wearables CVE ID : CVE-2021-1914	etins/august- 2021-bulletin	
Out-of- bounds Write	08-Sep-21	10	Possible buffer underflow due to lack of check for negative indices values when processing user provided input in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Voice & Music, Snapdragon Wearables CVE ID : CVE-2021-1916	https://www. qualcomm.co m/company/ product- security/bull etins/august- 2021-bulletin	H-QUA- WHS9- 170921/1861
Integer Underflow (Wrap or Wraparoun d)	08-Sep-21	10	Integer underflow can occur when the RTCP length is lesser than than the actual blocks present in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Voice & Music, Snapdragon Wearables CVE ID : CVE-2021-1919	https://www. qualcomm.co m/company/ product- security/bull etins/august- 2021-bulletin	H-QUA- WHS9- 170921/1862
Integer Underflow (Wrap or Wraparoun d)	08-Sep-21	10	Integer underflow can occur due to improper handling of incoming RTCP packets in Snapdragon Auto, Snapdragon Compute,	https://www. qualcomm.co m/company/ product- security/bull	H-QUA- WHS9- 170921/1863
CVSS Scoring Scale 0-1 1-2 2-3 3-4 4-5 5-6 6-7 7-8 8-9 9-10 Page 647 of 1474					

Page 647 of 1474

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID		
			Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Voice & Music, Snapdragon Wearables	etins/august- 2021-bulletin			
			CVE ID : CVE-2021-1920				
Incorrect Type Conversion or Cast	08-Sep-21	4.6	Incorrect pointer argument passed to trusted application TA could result in un- intended memory operations in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Industrial IOT	https://www. qualcomm.co m/company/ product- security/bull etins/august- 2021-bulletin	H-QUA- WHS9- 170921/1864		
			CVE ID : CVE-2021-1923				
wsa8810	wsa8810						
Exposure of Resource to Wrong Sphere	08-Sep-21	2.1	Child process can leak information from parent process due to numeric pids are getting compared and these pid can be reused in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wearables CVE ID : CVE-2021-1904	https://www. qualcomm.co m/company/ product- security/bull etins/august- 2021-bulletin	H-QUA-WSA8- 170921/1865		
Loop with Unreachable Exit Condition ('Infinite Loop')	08-Sep-21	5	Loop with unreachable exit condition may occur due to improper handling of unsupported input in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity,	https://www. qualcomm.co m/company/ product- security/bull etins/august- 2021-bulletin	H-QUA-WSA8- 170921/1866		
CVSS Scoring Scale 0-1 1-2 2-3 3-4 4-5 5-6 6-7 7-8 8-9 9-10 Page 648 of 1474							

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Voice & Music, Snapdragon Wearables CVE ID : CVE-2021-1914		
Out-of- bounds Write	08-Sep-21	10	Possible buffer underflow due to lack of check for negative indices values when processing user provided input in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Voice & Music, Snapdragon Wearables CVE ID : CVE-2021-1916	https://www. qualcomm.co m/company/ product- security/bull etins/august- 2021-bulletin	H-QUA-WSA8- 170921/1867
Integer Underflow (Wrap or Wraparoun d)	08-Sep-21	10	Integer underflow can occur when the RTCP length is lesser than than the actual blocks present in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Voice & Music, Snapdragon Wearables CVE ID : CVE-2021-1919	https://www. qualcomm.co m/company/ product- security/bull etins/august- 2021-bulletin	H-QUA-WSA8- 170921/1868
Integer Underflow (Wrap or Wraparoun d)	08-Sep-21	10	Integer underflow can occur due to improper handling of incoming RTCP packets in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT,	https://www. qualcomm.co m/company/ product- security/bull etins/august- 2021-bulletin	H-QUA-WSA8- 170921/1869
CVSS Scoring Sc	ale 0-1	1-2	2-3 3-4 4-5 5-6	6-7 7-8	8-9 9-10

Incorrect Type Conversion of CastImage: Superscript of Conversion Superscript of CastImage: Superscript of Conversion Superscript of Conversion Superscript of Conversion of CastImage: Superscript of Conversion Superscript of Conversion Superscript of Conversion Superscript of Conversion of CastSuperscript of Conversion Superscript of Conversion Sup	Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Incorrect Type Conversion or Cast08-Sep-21aIncorrect pointer argument passed to trusted application TA could result in un- intended memory operations Snapdragon Auto, Snapdragon Connectivity, Snapdragon Industrial IOT CVE ID : CVE-2021-1923https://www. qualcomm.co m/company/ product- scins/august- 2021-bulletinH-QUA-WSA8- 170921/1870Out-of- bounds Read08-Sep-21aBuffer over read could occur due to incorrect check of buffer size while flashing emmc devices in Snapdragon Consumer IOT, Snapdragon Mobile, Snapdragon Wearables, Snapdragon Wearables, Snapdragon Wearables, Snapdragon Wearables, Snapdragon Wearables, Snapdragon Wearables, Snapdragon Wearables, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networkinghttps://www. qualcomm.co m/company/ product- scurity/bull etins/august- 201-bulletinExposure of Resource to Wrong Sphere08-Sep-21aLack of strict validation of bootmode can lead to information disclosure in Snapdragon Compute, Snapdragon Compute, Snapdragon Consumer 10T, Snapdragon Compute, Networkinghttps://www. qualcomm.co m/company/ product- scurity/bull etins/august- 201-bulletinExposure of Resource to Wrong Sphere08-Sep-21ILack of strict validation of bootmode can lead to information disclosure in Snapdragon Consumer 10T, Snapdragon Consumer 10T, Snapdrago				Snapdragon IoT, Snapdragon Voice & Music, Snapdragon		
Incorrect Type Conversion or Cast08-Sep-214.6passed to trusted application 				CVE ID : CVE-2021-1920		
Out-of- bounds Read08-Sep-21a.6due to incorrect check of buffer size while flashing emmc devices in Snapdragon Consumer IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Voice & Wearables, Snapdragon Voice & Wearables, Snapdragon Voice & Veerables, Snapdragon Voice & Veerables, Snapdragon Voice & Networkinghttps://www. product- security/bull etins/august- 2021-bulletinHead POUA-WSA8- product- security/bull etins/august- 2021-bulletinHead POUA-WSA8- product- security/bull etins/august- 2021-bulletinHead POUA-WSA8- product- security/bull etins/august- 2021-bulletinHead POUA-WSA8- product- security/bull etins/august- 2021-bulletinHead POUA-WSA8- product- security/bull etins/august- 2021-bulletinHead POUA-WSA8- product- security/bull etins/august- 2021-bulletinHead POUA-WSA8- product- security/bull etins/august- 2021-bulletinHead POUA-WSA8- product- security/bull etins/august- 2021-bulletinHead POUA-WSA8- product- security/bull etins/august- 2021-bulletinHead POUA-WSA8- product- security/bull etins/august- 2021-bulletinHead POUA-WSA8- product- security/bull etins/august- 2021-bulletinHead POUA-WSA8- product- security/bull etins/august- 2021-bulletinHead POUA-WSA8- product- security/bull etins/august- 2021-bulletinHead POUA-WSA8- product- security/bull etins/august- 2021-bulletinHead POUA-WSA8- product- security/bull etins/august- 2021-bulletinExposure of Wrong Sphere08-Sep-212.1Excos of security/bull singdra	Type Conversion	08-Sep-21	4.6	passed to trusted application TA could result in un- intended memory operations in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Industrial IOT	qualcomm.co m/company/ product- security/bull etins/august-	
Exposure of Resource to Sphere08-Sep-212.1bootmode can lead to information disclosure in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wearableshttps://www. qualcomm.co m/company/ product- security/bull etins/august- 2021-bulletinH-QUA-WSA8- Product- security/bull etins/august- 2021-bulletin	bounds	08-Sep-21	3.6	due to incorrect check of buffer size while flashing emmc devices in Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking	qualcomm.co m/company/ product- security/bull etins/august-	•
	Resource to Wrong	08-Sep-21	2.1	bootmode can lead to information disclosure in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wearables	qualcomm.co m/company/ product- security/bull etins/august-	-

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Improper Restriction of Operations within the Bounds of a Memory Buffer	08-Sep-21	3.6	Possible out of bounds read due to incorrect validation of incoming buffer length in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile CVE ID : CVE-2021-1930	https://www. qualcomm.co m/company/ product- security/bull etins/august- 2021-bulletin	H-QUA-WSA8- 170921/1873
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	08-Sep-21	10	Possible buffer overflow due to improper validation of device types during P2P search in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Woice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking CVE ID : CVE-2021-1972	https://www. qualcomm.co m/company/ product- security/bull etins/august- 2021-bulletin	H-QUA-WSA8- 170921/1874
wsa8815					
Exposure of Resource to Wrong Sphere	08-Sep-21	2.1	Child process can leak information from parent process due to numeric pids are getting compared and these pid can be reused in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music,	https://www. qualcomm.co m/company/ product- security/bull etins/august- 2021-bulletin	H-QUA-WSA8- 170921/1875

CVSS Scoring Scale	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10
			P	age 651 c	of 1474					

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Snapdragon Wearables		
			CVE ID : CVE-2021-1904		
Loop with Unreachable Exit Condition ('Infinite Loop')	08-Sep-21	5	Loop with unreachable exit condition may occur due to improper handling of unsupported input in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Voice & Music, Snapdragon Wearables	https://www. qualcomm.co m/company/ product- security/bull etins/august- 2021-bulletin	H-QUA-WSA8- 170921/1876
			CVE ID : CVE-2021-1914		
Out-of- bounds Write	08-Sep-21	10	Possible buffer underflow due to lack of check for negative indices values when processing user provided input in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Voice & Music, Snapdragon Wearables CVE ID : CVE-2021-1916	https://www. qualcomm.co m/company/ product- security/bull etins/august- 2021-bulletin	H-QUA-WSA8- 170921/1877
Integer Underflow (Wrap or Wraparoun d)	08-Sep-21	10	Integer underflow can occur when the RTCP length is lesser than than the actual blocks present in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Voice & Music, Snapdragon	https://www. qualcomm.co m/company/ product- security/bull etins/august- 2021-bulletin	H-QUA-WSA8- 170921/1878

CVSS Scoring Scale

0-1

1-2

5-6

6-7

7-8

8-9

9-10

Integer Underflow (Wrap or Wraparoun d)08-Sep-2110Integer underflow can occur due to improper handling of incoming RTCP packets in Snapdragon Compute, Snapdragon Compute, Snapdragon Consumer 10T, Snapdragon Industrial 10T, Snapdragon Industrial 10T, Snapdragon Industrial 10T, Snapdragon Industrial 10T, Snapdragon Industrial 10T, Snapdragon Industrial 10T, Snapdragon Incometivity, Snapdragon Industrial 10T, Snapdragon Industrial 10T, Snapdragon Incometivity, Snapdragon Industrial 10T CVE ID : CVE-2021-1920https://www. qualcomm.co m/company/ product- security/bull etins/august- 2021/1880H-QUA-WSAB- 170921/1880Out-of- bounds Read08-Sep-213.6Buffer over read could occur due to incorrect check of butter size while flashing emmc devices in Snapdragon Nobile, Snapdragon Networking CVE ID : CVE-2021-1928https://www. qualcomm.co m/company/ product- security/bull etins/august- 2021-bulletinH-QUA-WSAB- H-QUA-WSAB- Industrial 107, Snapdragon Nobile, Snapdragon Nobile, Snapdragon Nobile, Snapdragon Networking CVE ID : CVE-2021-1928Https://www. qu	Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Integer Underflow (Wrap or W) (Wrap or (Wrap or (Wrap or Conversion or CastInteger Integer (Integer (Integer (Integer (Integer))Integer Integer (Integer) (Integer)Integer Integer (Integer) (Integer)Integer Integer (Integer) (Integer)Integer Integer (Integer) (Integer)Integer Integer (Integer) (Integer)Integer Integer)Integer (Integer) (Integer)Integer (Integer) (Integer)Integer (Integer) (Integer)Integer (Integer) (Integer)Integer (Integer) (Integer)Integer (Integer) (Integer)Integer (Integer) (Integer) (Integer)Integer (Integer) (Integer)Integer (Integer) (Integer) (Integer)Integer (Integer)				Wearables		
Integer Underflow (Wrap or Wraparoun d)08-Sep-21is and consumer is sandragon Consumer 10T, Snapdragon Consumer 10T, Snapdragon Consumer 10T, Snapdragon Consumer 10T, Snapdragon Consumer 10T, Snapdragon Industrial 10T, Snapdragon Industrial 10T, Snapdragon Industrial 10T, Snapdragon Industrial 10T, Snapdragon Consumer 10T, Snapdragon Industrial 10T, Snapdragon Consumer 10T, Snapdragon Industrial 10T, Snapdragon Compute, Snapdragon Compute, Snapdragon Consumer 10T, Snapdragon Compute, Snapdragon Consumer 10T, Snapdragon Consumer 10T, Snapdragon Compute, Snapdragon Consumer 10T, Snapdragon Consumer 10T, Snapdragon Consumer 10T, Snapdragon Compute, Snapdragon Consumer 10T, Snapdragon Consumer 10T, Snapdragon Consumer 10T, Snapdragon Notice, Snap				CVE ID : CVE-2021-1919		
Incorrect Type Conversion or Cast08-Sep-214.6Incorrect pointer argument passed to trusted application TA could result in un- insnapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Industrial IOThttps://www. product- security/bull etins/august- 2021-bulletinH-QUA-WSA8- 170921/1880Out-of- bounds Read08-Sep-213.6Buffer over read could occur due to incorrect check of buffer size while flashing emmc devices in Snapdragon Connectivity, Snapdragon Connectivity, Snapdragon Mobile, Snapdragon Voice & Mobile, Snapdragon Voice & Music, Snapdragon Voice & Music, Snapdragon Voice & Mobile, Snapdragon Voice & Music, Snapdragon Voice & Music, Snapdragon Voice & Music, Snapdragon Wired Infrastructure and Networkinghttps://www. qualcomm.co m/company/ product- security/bull etins/august- 2021-bulletinExposure of Resource to08-Sep-212.1Lack of strict validation of bottmode can lead tohttps://www. qualcomm.co	Underflow (Wrap or Wraparoun	08-Sep-21	10	due to improper handling of incoming RTCP packets in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Voice & Music, Snapdragon Wearables	qualcomm.co m/company/ product- security/bull etins/august-	•
Incorrect Type Conversion or Cast08-Sep-214.6passed to trusted application TA could result in un- intended memory operations in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Industrial IOThttps://www. qualcomm.co m/company/ product- security/bull etins/august- 2021-bulletinH-QUA-WSA8- 170921/1880Out-of- bounds Read08-Sep-218Buffer over read could occur due to incorrect check of buffer size while flashing emmc devices in Snapdragon Consumer IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Nobile, Snapdragon Verapdragon Verapdragon COSUMER IOT, Snapdragon Mobile, Snapdragon Worearables, Snapdragon 						
Out-of- bounds Read08-Sep-21adue to incorrect check of buffer size while flashing emmc devices in Snapdragon Connectivity, Snapdragon Mobile, Snapdragon Voice & Mobile, Snapdragon Voice & security/bull Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networkinghttps://www. qualcomm.co m/company/ product- security/bull etins/august- 2021-bulletinH-QUA-WSA8- Product- security/bull etins/august- 2021-bulletinExposure of Resource to08-Sep-212.1Lack of strict validation of bounds can lead tohttps://www. qualcomm.coH-QUA-WSA8- Product- security/bull etins/august- 2021-bulletin	Type Conversion	08-Sep-21	4.6	passed to trusted application TA could result in un- intended memory operations in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Industrial IOT	qualcomm.co m/company/ product- security/bull etins/august-	=
Resource to 00-Sep-21 2.1 bootmode can lead to qualcomm.co H-QUA-WSA8-	bounds	08-Sep-21	3.6	due to incorrect check of buffer size while flashing emmc devices in Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking	qualcomm.co m/company/ product- security/bull etins/august-	-
	-	08-Sep-21	2.1			H-QUA-WSA8-
					-	

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Wrong Sphere			information disclosure in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wearables CVE ID : CVE-2021-1929	m/company/ product- security/bull etins/august- 2021-bulletin	170921/1882
Improper Restriction of Operations within the Bounds of a Memory Buffer	08-Sep-21	3.6	Possible out of bounds read due to incorrect validation of incoming buffer length in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile CVE ID : CVE-2021-1930	https://www. qualcomm.co m/company/ product- security/bull etins/august- 2021-bulletin	H-QUA-WSA8- 170921/1883
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	08-Sep-21	10	Possible buffer overflow due to improper validation of device types during P2P search in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Woice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking CVE ID : CVE-2021-1972	https://www. qualcomm.co m/company/ product- security/bull etins/august- 2021-bulletin	H-QUA-WSA8- 170921/1884
wsa8830					
Exposure of Resource to Wrong	08-Sep-21	2.1	Child process can leak information from parent process due to numeric pids	https://www. qualcomm.co m/company/	H-QUA-WSA8- 170921/1885
CVSS Scoring Sca	ale 0-1	1-2	2-3 3-4 4-5 5-6 Page 654 of 1474	6-7 7-8	8-9 9-10

Page 654 of 1474

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Sphere			are getting compared and these pid can be reused in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables CVE ID : CVE-2021-1904	product- security/bull etins/august- 2021-bulletin	
Loop with Unreachable Exit Condition ('Infinite Loop')	08-Sep-21	5	Loop with unreachable exit condition may occur due to improper handling of unsupported input in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Voice & Music, Snapdragon Wearables CVE ID : CVE-2021-1914	https://www. qualcomm.co m/company/ product- security/bull etins/august- 2021-bulletin	H-QUA-WSA8- 170921/1886
Out-of- bounds Write	08-Sep-21	10	Possible buffer underflow due to lack of check for negative indices values when processing user provided input in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Voice & Music, Snapdragon Wearables CVE ID : CVE-2021-1916	https://www. qualcomm.co m/company/ product- security/bull etins/august- 2021-bulletin	H-QUA-WSA8- 170921/1887
	08-Sep-21	10	Integer underflow can occur	https://www.	H-QUA-WSA8-

Page 655 of 1474

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Underflow (Wrap or Wraparoun d)			when the RTCP length is lesser than than the actual blocks present in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Voice & Music, Snapdragon Wearables CVE ID : CVE-2021-1919	qualcomm.co m/company/ product- security/bull etins/august- 2021-bulletin	170921/1888
Integer Underflow (Wrap or Wraparoun d)	08-Sep-21	10	Integer underflow can occur due to improper handling of incoming RTCP packets in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Voice & Music, Snapdragon Wearables CVE ID : CVE-2021-1920	https://www. qualcomm.co m/company/ product- security/bull etins/august- 2021-bulletin	H-QUA-WSA8- 170921/1889
Incorrect Type Conversion or Cast	08-Sep-21	4.6	Incorrect pointer argument passed to trusted application TA could result in un- intended memory operations in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Industrial IOT CVE ID : CVE-2021-1923	https://www. qualcomm.co m/company/ product- security/bull etins/august- 2021-bulletin	H-QUA-WSA8- 170921/1890
Exposure of Resource to Wrong Sphere	08-Sep-21	2.1	Lack of strict validation of bootmode can lead to information disclosure in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity,	https://www. qualcomm.co m/company/ product- security/bull etins/august-	H-QUA-WSA8- 170921/1891

CVSS Scoring Scale

0-1

1-2 2-3

3-4

4-5

5-6

6-7

7-8

8-9

9-10

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wearables	2021-bulletin	
			CVE ID : CVE-2021-1929		
Improper Restriction of Operations within the Bounds of a Memory Buffer	08-Sep-21	3.6	Possible out of bounds read due to incorrect validation of incoming buffer length in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile	https://www. qualcomm.co m/company/ product- security/bull etins/august- 2021-bulletin	H-QUA-WSA8- 170921/1892
			CVE ID : CVE-2021-1930		
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	08-Sep-21	10	Possible buffer overflow due to improper validation of device types during P2P search in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Woice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking CVE ID : CVE-2021-1972	https://www. qualcomm.co m/company/ product- security/bull etins/august- 2021-bulletin	H-QUA-WSA8- 170921/1893
wsa8835	-			-	
Exposure of Resource to Wrong Sphere	08-Sep-21	2.1	Child process can leak information from parent process due to numeric pids are getting compared and these pid can be reused in Snapdragon Auto, Snapdragon Compute,	https://www. qualcomm.co m/company/ product- security/bull etins/august- 2021-bulletin	H-QUA-WSA8- 170921/1894
CVSS Scoring Sc	ale 0-1	1-2	2-3 3-4 4-5 5-6 Page 657 of 1474	6-7 7-8	8-9 9-10

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables		
			CVE ID : CVE-2021-1904		
Loop with Unreachable Exit Condition ('Infinite Loop')	08-Sep-21	5	Loop with unreachable exit condition may occur due to improper handling of unsupported input in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Voice & Music, Snapdragon Wearables CVE ID : CVE-2021-1914	https://www. qualcomm.co m/company/ product- security/bull etins/august- 2021-bulletin	H-QUA-WSA8- 170921/1895
			Possible buffer underflow		
Out-of- bounds Write	08-Sep-21	10	due to lack of check for negative indices values when processing user provided input in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Voice & Music, Snapdragon Wearables CVE ID : CVE-2021-1916	https://www. qualcomm.co m/company/ product- security/bull etins/august- 2021-bulletin	H-QUA-WSA8- 170921/1896
Integer Underflow (Wrap or Wraparoun d)	08-Sep-21	10	Integer underflow can occur when the RTCP length is lesser than than the actual blocks present in Snapdragon Auto, Snapdragon Compute,	https://www. qualcomm.co m/company/ product- security/bull	H-QUA-WSA8- 170921/1897
CVSS Scoring Sca	ale 0-1	1-2	2-3 3-4 4-5 5-6	6-7 7-8	8-9 9-10

Page 658 of 1474

Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
		Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Voice & Music, Snapdragon Wearables	etins/august- 2021-bulletin	
		CVE ID : CVE-2021-1919		
08-Sep-21	10	Integer underflow can occur due to improper handling of incoming RTCP packets in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Voice & Music, Snapdragon Wearables	https://www. qualcomm.co m/company/ product- security/bull etins/august- 2021-bulletin	H-QUA-WSA8- 170921/1898
		CVE ID : CVE-2021-1920		
08-Sep-21	4.6	Incorrect pointer argument passed to trusted application TA could result in un- intended memory operations in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Industrial IOT CVE ID : CVE-2021-1923	https://www. qualcomm.co m/company/ product- security/bull etins/august- 2021-bulletin	H-QUA-WSA8- 170921/1899
08-Sep-21	2.1	Lack of strict validation of bootmode can lead to information disclosure in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wearables	https://www. qualcomm.co m/company/ product- security/bull etins/august- 2021-bulletin	H-QUA-WSA8- 170921/1900
	08-Sep-21	08-Sep-21 10 08-Sep-21 4.6	08-Sep-2110Snapdragon Connectivity, Snapdragon Industrial IOT, Snapdragon Industrial IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Voice & Music, Snapdragon Wearables08-Sep-2110Integer underflow can occur due to improper handling of incoming RTCP packets in Snapdragon Auto, Snapdragon Compute, Snapdragon Iot, Snapdragon Snapdragon Iot, Snapdragon Voice & Music, Snapdragon Noite and the memory operations in Snapdragon Auto, Snapdragon Industrial IOT CVE ID : CVE-2021-192308-Sep-214.608-Sep-21Lack of strict validation of bootmode can lead to information disclosure in Snapdragon Connectivity, Snapdragon Connectivity, Snapdragon Connectivity, Snapdragon Industrial IOT, Snapdragon Industrial IOT, Snapdragon Industrial IOT, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Consumer IOT, Snapdragon Industrial	Image: Non-Stranger Standardon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Voice & Music, Snapdragon Wearablesetins/august- 2021-bulletin08-Sep-21110Integer underflow can occur due to improper handling of incoming RTCP packets in Snapdragon Consumer IOT, Snapdragon Consumer IOT, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Iot, Snapdragon Wearableshttps://www. qualcomm.co m/company/ product- security/bull etins/august- 2021-bulletin08-Sep-21110Incorrect pointer argument passed to trusted application in Snapdragon Compute, Snapdragon Compute, Snapdragon Industrial IOT, Snapdragon Compute, Snapdragon Industrial IOT Snapdragon Connectivity, Snapdragon Connectivity, Snapdragon Industrial IOT CVE ID : CVE-2021-1920https://www. qualcomm.co m/company/ product- security/bull etins/august- 2021-bulletin08-Sep-2114.6Incorrect pointer argument passed to trusted application in Snapdragon Connectivity, Snapdragon Industrial IOT Snapdragon Connectivity, Snapdragon Industrial IOT Snapdragon Connectivity, Snapdragon Industrial IOT Snapdragon Connectivity, Snapdragon Auto, Snapdragon Connectivity, Snapdragon Connectiv

 3-4
 4-5

 Page 659 of 1474

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2021-1929		
Improper Restriction of Operations within the Bounds of a Memory Buffer	08-Sep-21	3.6	Possible out of bounds read due to incorrect validation of incoming buffer length in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile CVE ID : CVE-2021-1930	https://www. qualcomm.co m/company/ product- security/bull etins/august- 2021-bulletin	H-QUA-WSA8- 170921/1901
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	08-Sep-21	10	Possible buffer overflow due to improper validation of device types during P2P search in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Woice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking CVE ID : CVE-2021-1972	https://www. qualcomm.co m/company/ product- security/bull etins/august- 2021-bulletin	H-QUA-WSA8- 170921/1902
Samsung					
h3					
Incorrect Authorizatio n	01-Sep-21	4.6	Samsung Drive Manager 2.0.104 on Samsung H3 devices allows attackers to bypass intended access controls on disk management. WideCharToMultiByte, WideCharStr, and MultiByteStr can contribute to password exposure.	N/A	H-SAM-H3- 170921/1903
CVSS Scoring Sc	ale 0-1	1-2	2-3 3-4 4-5 5-6 Page 660 of 1474	6-7 7-8	8-9 9-10

Page 660 of 1474

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2021-39373		
Schneider-el	ectric			L	L
accusine_pcs	n				
Exposure of Sensitive Information to an Unauthorize d Actor	02-Sep-21	6.5	A CWE-200: Exposure of Sensitive Information to an Unauthorized Actor vulnerability exist in AccuSine PCS+ / PFV+ (Versions prior to V1.6.7) and AccuSine PCSn (Versions prior to V2.2.4) that could allow an authenticated attacker to access the device via FTP protocol.	https://down load.schneide r- electric.com/f iles?p_Doc_Re f=SEVD- 2021-222-05	H-SCH-ACCU- 170921/1904
			CVE ID : CVE-2021-22793		
accusine_pcs	:\\+				
Exposure of Sensitive Information to an Unauthorize d Actor	02-Sep-21	6.5	A CWE-200: Exposure of Sensitive Information to an Unauthorized Actor vulnerability exist in AccuSine PCS+ / PFV+ (Versions prior to V1.6.7) and AccuSine PCSn (Versions prior to V2.2.4) that could allow an authenticated attacker to access the device via FTP protocol.	https://down load.schneide r- electric.com/f iles?p_Doc_Re f=SEVD- 2021-222-05	H-SCH-ACCU- 170921/1905
			CVE ID : CVE-2021-22793		
accusine_pfv	\\+				
Exposure of Sensitive Information to an Unauthorize d Actor	02-Sep-21	6.5	A CWE-200: Exposure of Sensitive Information to an Unauthorized Actor vulnerability exist in AccuSine PCS+ / PFV+ (Versions prior to V1.6.7) and AccuSine PCSn (Versions prior to V2.2.4) that could	https://down load.schneide r- electric.com/f iles?p_Doc_Re f=SEVD- 2021-222-05	H-SCH-ACCU- 170921/1906

 CVSS Scoring Scale
 0-1
 1-2
 2-3
 3-4
 4-5
 5-6
 6-7

 Page 661 of 1474

7-8

8-9

9-10

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			allow an authenticated attacker to access the device via FTP protocol.		
			CVE ID : CVE-2021-22793		
modicon_m3	40_bmxp341	000			
Improper Restriction of Operations within the Bounds of a Memory Buffer	02-Sep-21	4	A CWE-119: Improper Restriction of Operations within the Bounds of a Memory Buffer vulnerability that could cause a Denial of Service on the Modicon PLC controller / simulator when updating the controller application with a specially crafted project file exists in Modicon M580 CPU (part numbers BMEP* and BMEH*, all versions), Modicon M340 CPU (part numbers BMXP34*, all versions), Modicon MC80 (part numbers BMKC80*, all versions), Modicon Momentum Ethernet CPU (part numbers 171CBU*, all versions), PLC Simulator for EcoStruxure ^a Control Expert, including all Unity Pro versions (former name of EcoStruxure ^a Control Expert, all versions), PLC Simulator for EcoStruxure ^a Process Expert including all HDCS versions (former name of EcoStruxure ^a Process Expert, all versions), Modicon Quantum CPU (part numbers 140CPU*, all versions), Modicon Premium CPU (part	https://down load.schneide r- electric.com/f iles?p_Doc_Re f=SEVD- 2021-222-04	H-SCH-MODI- 170921/1907

CVSS Scoring Scale	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10
			P	age 662 c	of 1474					

Out-of- bounds Read02-Sep-214AACVE 1D: CVE-2021-22790Https://down load.schneide r echtroiter application with a specially crafted project file exists in Modicon MS80 CPU (part numbers BMKP34*, all versions), Modicon MS40 CPU (part numbers BMKC80*, all versions), Modicon MS40 CPU (part numbers BMKP34*, all versions), Modicon MS40 CPU (part numbers BMKC80*, all versions), Modicon MS40 CPU (part numbers BMKC80*, all versions), PLC Simulator for EcoStruxureª Control Expert, including all Unity Pro versions (former name of EcoStruxureª Process Expert including all Versions), PLC Simulator for EcoStruxureª Process Expert, all versions), Modicon Quantum CPU (part numbers 140CPU*, all versions), Modicon Premium CPU (part numbers) 140CPU*, all versions), Modicon Premium CPU (part numbers) Modicon Premium CPU (part numbers) Modicon Premium CPU (part numbers) 140CPU*, all versions), Modicon Premium CPU (part numbers) 170921/1909H-SCH-MODI- 170921/1909	Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Out-of-02-Sep-214A CWE-787: Out-of-boundshttps://downH-SCH-MODI- H-SCH-MODI-	Out-of- bounds			numbers TSXP5*, all versions). CVE ID : CVE-2021-22789 A CWE-125: Out-of-bounds Read vulnerability that could cause a Denial of Service on the Modicon PLC controller / simulator when updating the controller application with a specially crafted project file exists in Modicon M580 CPU (part numbers BMEP* and BMEH*, all versions), Modicon M340 CPU (part numbers BMXP34*, all versions), Modicon MC80 (part numbers BMKC80*, all versions), Modicon Momentum Ethernet CPU (part numbers 171CBU*, all versions), PLC Simulator for EcoStruxure ^a Control Expert, including all Unity Pro	https://down load.schneide r- electric.com/f iles?p_Doc_Re f=SEVD-	H-SCH-MODI-
02-Sep-21 4 110111/07104101 Doullas 110001/10011	Read			including all Unity Pro versions (former name of EcoStruxure ^a Control Expert, all versions), PLC Simulator for EcoStruxure ^a Process Expert including all HDCS versions (former name of EcoStruxure ^a Process Expert, all versions), Modicon Quantum CPU (part numbers 140CPU*, all versions), Modicon Premium CPU (part numbers TSXP5*, all versions).	f=SEVD-	
		02-Sep-21	4			

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Write			cause a Denial of Service on the Modicon PLC controller / simulator when updating the controller application with a specially crafted project file exists in Modicon M580 CPU (part numbers BMEP* and BMEH*, all versions), Modicon M340 CPU (part numbers BMXP34*, all versions), Modicon MC80 (part numbers BMKC80*, all versions), Modicon MC80 (part numbers 171CBU*, all versions), PLC Simulator for EcoStruxure ^a Control Expert, including all Unity Pro versions (former name of EcoStruxure ^a Control Expert, all versions), PLC Simulator for EcoStruxure ^a Process Expert including all HDCS versions (former name of EcoStruxure ^a Process Expert, all versions), Modicon Quantum CPU (part numbers 140CPU*, all versions), Modicon Premium CPU (part numbers TSXP5*, all versions).	r- electric.com/f iles?p_Doc_Re f=SEVD- 2021-222-04	
NULL Pointer Dereference CVSS Scoring Sc	02-Sep-21	5	A CWE-476: NULL Pointer Dereference vulnerability that could cause a Denial of Service on the Modicon PLC controller / simulator when updating the controller application with a specially crafted project file exists in	https://down load.schneide r- electric.com/f iles?p_Doc_Re f=SEVD- 2021-222-04	H-SCH-MODI- 170921/1910 8-9 9-10

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Modicon M580 CPU (part numbers BMEP* and BMEH*, all versions), Modicon M340 CPU (part numbers BMXP34*, all versions), Modicon MC80 (part numbers BMKC80*, all versions), Modicon Momentum Ethernet CPU (part numbers 171CBU*, all versions), PLC Simulator for EcoStruxure ^a Control Expert, including all Unity Pro versions (former name of EcoStruxure ^a Control Expert, all versions), PLC Simulator for EcoStruxure ^a Process Expert including all HDCS versions (former name of EcoStruxure ^a Process Expert, all versions), Modicon Quantum CPU (part numbers 140CPU*, all versions), Modicon Premium CPU (part numbers TSXP5*, all versions).		
modicon_m3	40_bmxp342	010			
Improper Restriction of Operations within the Bounds of a Memory Buffer	02-Sep-21	4	A CWE-119: Improper Restriction of Operations within the Bounds of a Memory Buffer vulnerability that could cause a Denial of Service on the Modicon PLC controller / simulator when updating the controller application with a specially crafted project file exists in Modicon M580 CPU (part	https://down load.schneide r- electric.com/f iles?p_Doc_Re f=SEVD- 2021-222-04	H-SCH-MODI- 170921/1911

CVSS Scoring Scale	0-1	1-2	2-3	5-4	4-5	5-0	6-7	7-8	0-9	9-10
CVCC Cooring Coolo	0.1	1 0	n n	2.4	4 F	ГС	67	70	0.0	0.10

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			numbers BMEP* and BMEH*, all versions), Modicon M340 CPU (part numbers BMXP34*, all versions), Modicon MC80 (part numbers BMKC80*, all versions), Modicon Momentum Ethernet CPU (part numbers 171CBU*, all versions), PLC Simulator for EcoStruxure ^a Control Expert, including all Unity Pro versions (former name of EcoStruxure ^a Control Expert, all versions), PLC Simulator for EcoStruxure ^a Process Expert including all HDCS versions (former name of EcoStruxure ^a Process Expert, all versions), Modicon Quantum CPU (part numbers 140CPU*, all versions), Modicon Premium CPU (part numbers TSXP5*, all versions). CVE ID : CVE-2021-22789		
Out-of- bounds Read	02-Sep-21	4	A CWE-125: Out-of-bounds Read vulnerability that could cause a Denial of Service on the Modicon PLC controller / simulator when updating the controller application with a specially crafted project file exists in Modicon M580 CPU (part numbers BMEP* and BMEH*, all versions), Modicon M340 CPU (part numbers BMXP34*, all versions), Modicon MC80 (part numbers BMKC80*, all	https://down load.schneide r- electric.com/f iles?p_Doc_Re f=SEVD- 2021-222-04	H-SCH-MODI- 170921/1912
CVSS Scoring Sc	ale 0-1	1-2	2-3 3-4 4-5 5-6	6-7 7-8	8-9 9-10

			versions), Modicon Momentum Ethernet CPU (part numbers 171CBU*, all versions), PLC Simulator for EcoStruxure ^a Control Expert, including all Unity Pro versions (former name of EcoStruxure ^a Control Expert, all versions), PLC Simulator for EcoStruxure ^a Process Expert including all HDCS versions (former name of EcoStruxure ^a Process Expert, all versions), Modicon Quantum CPU (part numbers 140CPU*, all versions), Modicon Premium CPU (part numbers TSXP5*, all versions).		
Out-of- bounds Write	02-Sep-21	4	A CWE-787: Out-of-bounds Write vulnerability that could cause a Denial of Service on the Modicon PLC controller / simulator when updating the controller application with a specially crafted project file exists in Modicon M580 CPU (part numbers BMEP* and BMEH*, all versions), Modicon M340 CPU (part numbers BMXP34*, all versions), Modicon MC80 (part numbers BMKC80*, all versions), Modicon Momentum Ethernet CPU (part numbers 171CBU*, all versions), PLC Simulator for EcoStruxure ^a Control Expert, including all Unity Pro	https://down load.schneide r- electric.com/f iles?p_Doc_Re f=SEVD- 2021-222-04	H-SCH-MODI- 170921/1913

Page 667 of 1474

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			versions (former name of EcoStruxure ^ª Control Expert, all versions), PLC Simulator for EcoStruxure ^ª Process Expert including all HDCS versions (former name of EcoStruxure ^ª Process Expert, all versions), Modicon Quantum CPU (part numbers 140CPU*, all versions), Modicon Premium CPU (part numbers TSXP5*, all versions). CVE ID : CVE-2021-22791		
NULL Pointer Dereference	02-Sep-21	5	A CWE-476: NULL Pointer Dereference vulnerability that could cause a Denial of Service on the Modicon PLC controller / simulator when updating the controller application with a specially crafted project file exists in Modicon M580 CPU (part numbers BMEP* and BMEH*, all versions), Modicon M340 CPU (part numbers BMXP34*, all versions), Modicon MC80 (part numbers BMKC80*, all versions), Modicon Momentum Ethernet CPU (part numbers 171CBU*, all versions), PLC Simulator for EcoStruxure ^a Control Expert, including all Unity Pro versions (former name of EcoStruxure ^a Control Expert, all versions), PLC Simulator for EcoStruxure ^a Process Expert including all HDCS	https://down load.schneide r- electric.com/f iles?p_Doc_Re f=SEVD- 2021-222-04	H-SCH-MODI- 170921/1914
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 & CVE ID	Patch	NCIIPC ID
			versions (former name of EcoStruxure ^a Process Expert, all versions), Modicon Quantum CPU (part numbers 140CPU*, all versions), Modicon Premium CPU (part numbers TSXP5*, all versions). CVE ID : CVE-2021-22792		
modicon_m3	40_bmxp342	020			
Improper Restriction of Operations within the Bounds of a Memory Buffer	02-Sep-21	4	A CWE-119: Improper Restriction of Operations within the Bounds of a Memory Buffer vulnerability that could cause a Denial of Service on the Modicon PLC controller / simulator when updating the controller application with a specially crafted project file exists in Modicon M580 CPU (part numbers BMEP* and BMEH*, all versions), Modicon M340 CPU (part numbers BMXP34*, all versions), Modicon MC80 (part numbers BMKC80*, all versions), Modicon Momentum Ethernet CPU (part numbers 171CBU*, all versions), PLC Simulator for EcoStruxure ^a Control Expert, including all Unity Pro versions (former name of EcoStruxure ^a Process Expert including all HDCS versions (former name of	https://down load.schneide r- electric.com/f iles?p_Doc_Re f=SEVD- 2021-222-04	H-SCH-MODI- 170921/1915

CVSS Scoring Scale	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10
			р		f 1 1 7 1					

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			EcoStruxure ^a Process Expert, all versions), Modicon Quantum CPU (part numbers 140CPU*, all versions), Modicon Premium CPU (part numbers TSXP5*, all versions).		
			CVE ID : CVE-2021-22789		
Out-of- bounds Read	02-Sep-21	4	A CWE-125: Out-of-bounds Read vulnerability that could cause a Denial of Service on the Modicon PLC controller / simulator when updating the controller application with a specially crafted project file exists in Modicon M580 CPU (part numbers BMEP* and BMEH*, all versions), Modicon M340 CPU (part numbers BMXP34*, all versions), Modicon MC80 (part numbers BMKC80*, all versions), Modicon Momentum Ethernet CPU (part numbers 171CBU*, all versions), PLC Simulator for EcoStruxure ^a Control Expert, including all Unity Pro versions (former name of EcoStruxure ^a Control Expert, all versions), PLC Simulator for EcoStruxure ^a Process Expert including all HDCS versions (former name of EcoStruxure ^a Process Expert, all versions), Modicon Quantum CPU (part numbers 140CPU*, all versions), Modicon Premium CPU (part numbers TSXP5*, all	https://down load.schneide r- electric.com/f iles?p_Doc_Re f=SEVD- 2021-222-04	H-SCH-MODI- 170921/1916
CVSS Scoring Sc	ale 0-1	1-2	2-3 3-4 4-5 5-6	6-7 7-8	8-9 9-10

Out-of- bounds WriteQ2-Sep-214A CWE-107: CVE-2021-22790https://down load.schneidhttps://down load.schneidOut-of- bounds Write02-Sep-214A CWE-787: Out-of-bounds Write vulnerability that could cause a Denial of Service on aspecially crafted project file exists in Modicon PLC controller / simulator when updating the controller application with a specially crafted project file exists in Modicon M580 CPU (part numbers BMEP* and BMEH*, all versions), Modicon M680 (part numbers BMKC90*, all versions), Modicon MC80 (part numbers T1/CBU*, all versions), PLC Simulator for EcoStruxure* Control Expert, all versions), PLC Simulator for EcoStruxure* Process Expert including all Unity Pro versions (former name of EcoStruxure* Process Expert including all Unity Pro versions), Modicon Modicon P201 P201-222-04H-SCH-MODI- 170921/1917NULL Pointer Pointer Pointer Pointer02-Sep-215A CWE-476: NULL Pointer Dereference vulnerability that could cause a Denial of Ereferencehttps://down load.schneid r-	Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Out-of- bounds02-Sep-214A CWE-787: Out-of-bounds Write vulnerability that could cause a Denial of Service on the Modicon PLC controller / simulator when updating the exists in Modicon MS80 CPU (part numbers BMEP* and BMEH*, all versions), Modicon M340 CPU (part numbers BMK2630*, all versions), Modicon MC80 (part numbers BMK2630*, all versions), PLC Simulator for EcoStruxure* Control Expert, including all Unity Pro versions), PLC Simulator for EcoStruxure* Control Expert, all versions), PLC Simulator for EcoStruxure* Control Expert, all versions), PLC Simulator for EcoStruxure* Control Expert, all versions), PLC Simulator for EcoStruxure* Process Expert including all HDCS versions (former name of EcoStruxure* Process Expert, all versions), PLC Simulator for EcoStruxure* Process Expert including all HDCS versions (former name of EcoStruxure* Process Expert, all versions), Modicon Quantum CPU (part numbers 140CPU*, all versions), Modicon Premium CPU (part numbers TSXP5*, all versions)https://down lH-SCH-MODI- 170921/1917NULL Pointer02-Sep-215A CWE-476: NULL Pointer Dereference vulnerabilityhttps://down load.schneideH-SCH-MODI- 170921/1918				versions).		
Out-of- bounds02-Sep-214A cause a Denial of Service on the Modicon PLC controller / simulator when updating the controller application with a specially crafted project file exists in Modicon M580 CPU (part numbers BMEP* and BMEH*, all versions), Modicon M340 CPU (part numbers BMEP* and BMEH*, all versions), Modicon M580 CPU (part numbers BMEP* and BMEH*, all versions), Modicon M580 CPU (part numbers BMK208*, all versions), Modicon M280 exists in including all Unity Pro versions), PLC Simulator for EcoStruxure ^a Control Expert, all versions), PLC Simulator for for EcoStruxure ^a Control Expert, all versions), Modicon Quantum CPU (part numbers 140 CPU*, all versions), Modicon versions, PLC Simulator for for EcoStruxure ^a Control Expert, all versions), Modicon Quantum CPU (part numbers 140 CPU*, all versions), Modicon Nodicon Premium CPU (part numbers 140 CPU*, all versions), Modicon 140 CPU*, all versions), Mo				CVE ID : CVE-2021-22790		
Pointer02-Sep-215Dereference vulnerabilityInteps// downH-SCH-MODI- 170921/1918	bounds	02-Sep-21	4	Write vulnerability that could cause a Denial of Service on the Modicon PLC controller / simulator when updating the controller application with a specially crafted project file exists in Modicon M580 CPU (part numbers BMEP* and BMEH*, all versions), Modicon M340 CPU (part numbers BMXP34*, all versions), Modicon MC80 (part numbers BMKC80*, all versions), Modicon Momentum Ethernet CPU (part numbers 171CBU*, all versions), PLC Simulator for EcoStruxure ^a Control Expert, including all Unity Pro versions (former name of EcoStruxure ^a Control Expert, all versions), PLC Simulator for EcoStruxure ^a Process Expert including all HDCS versions (former name of EcoStruxure ^a Process Expert, all versions), Modicon Quantum CPU (part numbers 140CPU*, all versions), Modicon Premium CPU (part numbers TSXP5*, all versions).	load.schneide r- electric.com/f iles?p_Doc_Re f=SEVD-	
	Pointer	02-Sep-21	5	Dereference vulnerability	load.schneide	

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Service on the Modicon PLC	electric.com/f	
			controller / simulator when	iles?p_Doc_Re	
			updating the controller	f=SEVD-	
			application with a specially	2021-222-04	
			crafted project file exists in		
			Modicon M580 CPU (part		
			numbers BMEP* and BMEH*,		
			all versions), Modicon M340		
			CPU (part numbers		
			BMXP34*, all versions),		
			Modicon MC80 (part		
			numbers BMKC80*, all		
			versions), Modicon		
			Momentum Ethernet CPU		
			(part numbers 171CBU*, all		
			versions), PLC Simulator for		
			EcoStruxure ^a Control Expert,		
			including all Unity Pro		
			versions (former name of		
			EcoStruxure ^a Control Expert,		
			all versions), PLC Simulator		
			for EcoStruxure ^a Process		
			Expert including all HDCS		
			versions (former name of		
			EcoStruxure ^a Process Expert,		
			all versions), Modicon		
			Quantum CPU (part numbers		
			140CPU*, all versions),		
			Modicon Premium CPU (part		
			numbers TSXP5*, all		
			versions).		
			CVE ID : CVE-2021-22792		
modicon_m3	40_bmxp342	030			
Improper			A CWE-119: Improper	https://down	
Restriction			Restriction of Operations	load.schneide	
of	02 500 21	4	within the Bounds of a	r-	H-SCH-MODI-
Operations	02-Sep-21	4	Memory Buffer vulnerability	electric.com/f	170921/1919
within the			that could cause a Denial of	iles?p_Doc_Re	
Bounds of a			Service on the Modicon PLC	f=SEVD-	
	l				

CVSS Scoring Scale	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10
			Pa	age 672 c	of 1474					

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Memory Buffer			controller / simulator when updating the controller application with a specially crafted project file exists in Modicon M580 CPU (part numbers BMEP* and BMEH*, all versions), Modicon M340 CPU (part numbers BMXP34*, all versions), Modicon MC80 (part numbers BMKC80*, all versions), Modicon Momentum Ethernet CPU (part numbers 171CBU*, all versions), PLC Simulator for EcoStruxure ^a Control Expert, including all Unity Pro versions (former name of EcoStruxure ^a Control Expert, all versions), PLC Simulator for EcoStruxure ^a Process Expert including all HDCS versions (former name of EcoStruxure ^a Process Expert, all versions), Modicon Quantum CPU (part numbers 140CPU*, all versions), Modicon Premium CPU (part numbers TSXP5*, all versions). CVE ID : CVE-2021-22789	2021-222-04	
Out-of- bounds Read CVSS Scoring Sc	02-Sep-21 ale 0-1	4	A CWE-125: Out-of-bounds Read vulnerability that could cause a Denial of Service on the Modicon PLC controller / simulator when updating the controller application with a specially crafted project file exists in Modicon M580 CPU (part numbers BMEP* and 2-3 3-4 4-5 5-6	https://down load.schneide r- electric.com/f iles?p_Doc_Re f=SEVD- 2021-222-04	H-SCH-MODI- 170921/1920 8-9 9-10

Out-of- bounds 02-Sep-21 4 BMEH*, all versions), Modicon M240 CPU (part numbers BMXP34*, all versions), Modicon MC80 (part numbers BMKC80*, all versions), Modicon Wutter (part numbers 171CBU*, all versions), PLC Simulator for EcoStruxure* Control Expert, all versions), PLC Simulator for EcoStruxure* Process Expert including all HDCS versions (former name of EcoStruxure* Process Expert, all versions), Modicon Quantum CPU (part numbers 140CPU*, all versions), Write 1 02-Sep-21 A CWE-787: Out-of-bounds Write vulnerability that could cause a Denial of Service on the Modicon PLC controller / simulator when updating the controller application with a specially crafted project file exists in Modicon M580 CPU (part numbers BMEP* and BMEH*, all versions), Modicon M340 CPU (part numbers BMKP34*, all versions), Modicon M280 (part numbers BMKP34*, all versions), Modicon M280 (part numbers BMKC80*, all versions), Modicon M280 H-SCH-MODI- 170921/1921	Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Out-of- bounds02-Sep-214Write vulnerability that could cause a Denial of Service on the Modicon PLC controller / simulator when updating the controller application with a specially crafted project file exists in Modicon M580 CPU (part numbers BMEP* and BMEH*, all versions), Modicon M340 CPU (part numbers BMXP34*, all versions), Modicon MC80 (part numbers BMKC80*, allH-SCH-MODI- H-SCH-MODI- 170921/1921				Modicon M340 CPU (part numbers BMXP34*, all versions), Modicon MC80 (part numbers BMKC80*, all versions), Modicon Momentum Ethernet CPU (part numbers 171CBU*, all versions), PLC Simulator for EcoStruxure ^a Control Expert, including all Unity Pro versions (former name of EcoStruxure ^a Control Expert, all versions), PLC Simulator for EcoStruxure ^a Process Expert including all HDCS versions (former name of EcoStruxure ^a Process Expert, all versions), Modicon Quantum CPU (part numbers 140CPU*, all versions), Modicon Premium CPU (part numbers TSXP5*, all versions).		
	bounds	02-Sep-21	4	Write vulnerability that could cause a Denial of Service on the Modicon PLC controller / simulator when updating the controller application with a specially crafted project file exists in Modicon M580 CPU (part numbers BMEP* and BMEH*, all versions), Modicon M340 CPU (part numbers BMXP34*, all versions), Modicon MC80	load.schneide r- electric.com/f iles?p_Doc_Re f=SEVD-	

Page 674 of 1474

Pointer 02-Sen-21 5 all voncional Madican M240 electric com/f	Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
NULLDereference vulnerability that could cause a Denial of Service on the Modicon PLC controller / simulator when updating the controller application with a specially crafted project file exists in Modicon M580 CPU (part load.schneide enumbers BMEP* and BMEH*, iles?p_Doc_Re f=SEVD- 2021-222-04 Modicon MC80 (part numbers BMKC80*, all versions), Modicon Momentum Ethernet CPU (part numbers 171CBU*, allHttps://down load.schneide f=SEVD- 2021-222-04H- H- 17				(part numbers 171CBU*, all versions), PLC Simulator for EcoStruxure ^a Control Expert, including all Unity Pro versions (former name of EcoStruxure ^a Control Expert, all versions), PLC Simulator for EcoStruxure ^a Process Expert including all HDCS versions (former name of EcoStruxure ^a Process Expert, all versions), Modicon Quantum CPU (part numbers 140CPU*, all versions), Modicon Premium CPU (part numbers TSXP5*, all versions).		
EcoStruxure ^a Control Expert, including all Unity Pro	Pointer	02-Sep-21	5	Dereference vulnerability that could cause a Denial of Service on the Modicon PLC controller / simulator when updating the controller application with a specially crafted project file exists in Modicon M580 CPU (part numbers BMEP* and BMEH*, all versions), Modicon M340 CPU (part numbers BMXP34*, all versions), Modicon MC80 (part numbers BMKC80*, all versions), Modicon Momentum Ethernet CPU (part numbers 171CBU*, all versions), PLC Simulator for EcoStruxure ^a Control Expert,	load.schneide r- electric.com/f iles?p_Doc_Re f=SEVD-	H-SCH-MODI- 170921/1922

Page 675 of 1474

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			versions (former name of EcoStruxure ^a Control Expert, all versions), PLC Simulator for EcoStruxure ^a Process Expert including all HDCS versions (former name of EcoStruxure ^a Process Expert, all versions), Modicon Quantum CPU (part numbers 140CPU*, all versions), Modicon Premium CPU (part numbers TSXP5*, all versions). CVE ID : CVE-2021-22792		
modicon_m5	80_bmeh582	040			
Improper Restriction of Operations within the Bounds of a Memory Buffer	02-Sep-21	4	A CWE-119: Improper Restriction of Operations within the Bounds of a Memory Buffer vulnerability that could cause a Denial of Service on the Modicon PLC controller / simulator when updating the controller application with a specially crafted project file exists in Modicon M580 CPU (part numbers BMEP* and BMEH*, all versions), Modicon M340 CPU (part numbers BMXP34*, all versions), Modicon MC80 (part numbers BMKC80*, all versions), Modicon Momentum Ethernet CPU (part numbers 171CBU*, all versions), PLC Simulator for EcoStruxure ^a Control Expert, including all Unity Pro versions (former name of	https://down load.schneide r- electric.com/f iles?p_Doc_Re f=SEVD- 2021-222-04	H-SCH-MODI- 170921/1923

CVSS Scoring Scale	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10
			р	aga 676 g	£1474					

Out-of- bounds 02-Sep-21 4 Read A CWE-125: Out-of-bounds resions), PLC Simulator for EcoStruxure ^a Process Expert including all HDCS versions), Modicon Quantum CPU (part numbers 140CPU*, all versions), Modicon Premium CPU (part numbers TSXP5*, all versions). Items: CVE ID : CVE-2021-22789 A CWE-125: Out-of-bounds Read vulnerability that could cause a Denial of Service on the Modicon PLC controller / simulator when updating the controller application with a specially crafted project file exists in Modicon MSB0 CPU (part numbers BMKP3*, all versions), Modicon Momentum Ethernet CPU (part numbers BMKP3*, all versions), Modicon MGB0 CPU (part numbers BMKP3*, all versions), Modicon MGB0 CPU (part numbers BMKP3*, all versions), PLC Simulator for EcoStruxure* Control Expert, all versions), PLC Simulator for EcoStruxure* Control Expert, all versions), PLC Simulator for EcoStruxure* Process Expert including all HDCS versions (former name of EcoStruxure* Process Expert including all HDCS versions (former name of EcoStruxure* Process H-SCH-MODI- 170921/1924	Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Out-of- bounds02-Sep-214Read vulnerability that could cause a Denial of Service on the Modicon PLC controller / simulator when updating the controller application with a specially crafted project file exists in Modicon M580 CPU (part numbers BMEP* and BMEH*, all versions), Modicon M340 CPU (part numbers BMXP34*, all versions), Modicon MC80https://down load.schneideH-SCH-MODI- 170921/1924Read02-Sep-214Mether a ll versions), Modicon MC80 (part numbers BMKC80*, all versions), Modicon MC80 (part numbers BMKC80*, all versions), Modicon for EcoStruxureª Control Expert, all versions), PLC Simulator for EcoStruxureª Control Expert, all versions), PLC Simulator for EcoStruxureª Process Expert including all HDCS versions (former name of EcoStruxureª Process Expert,H-SCH-MODI- 170921/1924				all versions), PLC Simulator for EcoStruxure ^a Process Expert including all HDCS versions (former name of EcoStruxure ^a Process Expert, all versions), Modicon Quantum CPU (part numbers 140CPU*, all versions), Modicon Premium CPU (part numbers TSXP5*, all versions).		
	bounds Read			A CWE-125: Out-of-bounds Read vulnerability that could cause a Denial of Service on the Modicon PLC controller / simulator when updating the controller application with a specially crafted project file exists in Modicon M580 CPU (part numbers BMEP* and BMEH*, all versions), Modicon M340 CPU (part numbers BMXP34*, all versions), Modicon MC80 (part numbers BMKC80*, all versions), Modicon Momentum Ethernet CPU (part numbers 171CBU*, all versions), PLC Simulator for EcoStruxure ^a Control Expert, including all Unity Pro versions (former name of EcoStruxure ^a Control Expert, all versions), PLC Simulator for EcoStruxure ^a Process Expert including all HDCS versions (former name of	load.schneide r- electric.com/f iles?p_Doc_Re f=SEVD- 2021-222-04	170921/1924

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			all versions), Modicon Quantum CPU (part numbers 140CPU*, all versions), Modicon Premium CPU (part numbers TSXP5*, all versions). CVE ID : CVE-2021-22790		
Out-of- bounds Write	02-Sep-21	4	A CWE-787: Out-of-bounds Write vulnerability that could cause a Denial of Service on the Modicon PLC controller / simulator when updating the controller application with a specially crafted project file exists in Modicon M580 CPU (part numbers BMEP* and BMEH*, all versions), Modicon M340 CPU (part numbers BMXP34*, all versions), Modicon MC80 (part numbers BMKC80*, all versions), Modicon Momentum Ethernet CPU (part numbers 171CBU*, all versions), PLC Simulator for EcoStruxure ^a Control Expert, including all Unity Pro versions (former name of EcoStruxure ^a Control Expert, all versions), PLC Simulator for EcoStruxure ^a Process Expert including all HDCS versions (former name of EcoStruxure ^a Process Expert, all versions), Modicon Quantum CPU (part numbers 140CPU*, all versions), Modicon Premium CPU (part numbers TSXP5*, all	https://down load.schneide r- electric.com/f iles?p_Doc_Re f=SEVD- 2021-222-04	H-SCH-MODI- 170921/1925

CVSS Scoring Scale	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10
Page 678 of 1474										

			versions).		
			CVE ID : CVE-2021-22791		
NULL Pointer Dereference	02-Sep-21	5	A CWE-476: NULL Pointer Dereference vulnerability that could cause a Denial of Service on the Modicon PLC controller / simulator when updating the controller application with a specially crafted project file exists in Modicon M580 CPU (part numbers BMEP* and BMEH*, all versions), Modicon M340 CPU (part numbers BMXP34*, all versions), Modicon MC80 (part numbers BMKC80*, all versions), Modicon Momentum Ethernet CPU (part numbers 171CBU*, all versions), PLC Simulator for EcoStruxure ^a Control Expert, including all Unity Pro versions (former name of EcoStruxure ^a Control Expert, all versions), PLC Simulator for EcoStruxure ^a Process Expert including all HDCS versions (former name of EcoStruxure ^a Process Expert, all versions), Modicon Quantum CPU (part numbers 140CPU*, all versions), Modicon Premium CPU (part numbers TSXP5*, all versions).	https://down load.schneide r- electric.com/f iles?p_Doc_Re f=SEVD- 2021-222-04	H-SCH-MODI- 170921/1926

CVSS Scoring Scale	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10
			D	200 670 0	f 1/7/					

Improper Restriction of Operations within the Bounds of a Memory Buffer vulnerability that could cause a Denial of Service on the Modicon PLC controller / simulator when updating the controller application with a specially crafted project file exists in Modicon M580 CPU (part numbers BMEP* and BMEH*, all versions), Modicon M580 CPU (part numbers BMEP* and BMEH*, all versions), Modicon M580 CPU (part numbers BMK284*, all versions), Modicon M580 CPU (part numbers BMK280*, all versions), Modicon M580 CPU (part numbers BMK280*, all versions), Modicon M580 CPU (part numbers BMK280*, all versions), Modicon M580 CPU (part numbers BMK280*, all versions), PLC Simulator for EcoStruxure ^a Control Expert, all versions), PLC Simulator for EcoStruxure ^a Control Expert, all versions), PLC Simulator for EcoStruxure ^a Control Expert, all versions), Modicon Quantum CPU (part numbers I ACOEP1 (part numbers T3CP5*, all versions). CVE ID : CVE-2021-22789H-SCH-MODI- 170921/1928Out-of- bounds02-Sep-214A CWE-125: Out-of-bounds Read vulnerability that could cause a Denial of Service on for Service on for Secostruxurea Process Expert including all HDCS versions). Modicon Premium CPU (part numbers 140CPI*, all versions), Modicon Premium CPU (part numbers 140CPI*,	Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Out-of- bounds 02-Sep-21 4 Read vulnerability that could load.schneide 170921/1928	Restriction of Operations within the Bounds of a Memory	02-Sep-21	4	Restriction of Operations within the Bounds of a Memory Buffer vulnerability that could cause a Denial of Service on the Modicon PLC controller / simulator when updating the controller application with a specially crafted project file exists in Modicon M580 CPU (part numbers BMEP* and BMEH*, all versions), Modicon M340 CPU (part numbers BMXP34*, all versions), Modicon MC80 (part numbers BMKC80*, all versions), Modicon Momentum Ethernet CPU (part numbers 171CBU*, all versions), PLC Simulator for EcoStruxure ^a Control Expert, including all Unity Pro versions (former name of EcoStruxure ^a Control Expert, all versions), PLC Simulator for EcoStruxure ^a Process Expert including all HDCS versions (former name of EcoStruxure ^a Process Expert, all versions), Modicon Quantum CPU (part numbers 140CPU*, all versions), Modicon Premium CPU (part numbers TSXP5*, all versions).	load.schneide r- electric.com/f iles?p_Doc_Re f=SEVD-	
		02-Sep-21	4	Read vulnerability that could	load.schneide	

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Read			the Modicon PLC controller / simulator when updating the controller application with a specially crafted project file exists in Modicon M580 CPU (part numbers BMEP* and BMEH*, all versions), Modicon M340 CPU (part numbers BMXP34*, all versions), Modicon MC80 (part numbers BMKC80*, all versions), Modicon MC80 (part numbers BMKC80*, all versions), Modicon Momentum Ethernet CPU (part numbers 171CBU*, all versions), PLC Simulator for EcoStruxure ^a Control Expert, including all Unity Pro versions (former name of EcoStruxure ^a Control Expert, all versions), PLC Simulator for EcoStruxure ^a Process Expert including all HDCS versions (former name of EcoStruxure ^a Process Expert, all versions), Modicon Quantum CPU (part numbers 140CPU*, all versions), Modicon Premium CPU (part numbers TSXP5*, all versions).	electric.com/f iles?p_Doc_Re f=SEVD- 2021-222-04	
Out-of- bounds Write CVSS Scoring Sc	02-Sep-21 ale 0-1	4	A CWE-787: Out-of-bounds Write vulnerability that could cause a Denial of Service on the Modicon PLC controller / simulator when updating the controller application with a specially crafted project file exists in Modicon M580 CPU (part numbers BMEP* and	https://down load.schneide r- electric.com/f iles?p_Doc_Re f=SEVD- 2021-222-04	H-SCH-MODI- 170921/1929 8-9 9-10

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			BMEH*, all versions), Modicon M340 CPU (part numbers BMXP34*, all versions), Modicon MC80 (part numbers BMKC80*, all versions), Modicon Momentum Ethernet CPU (part numbers 171CBU*, all versions), PLC Simulator for EcoStruxure ^a Control Expert, including all Unity Pro versions (former name of EcoStruxure ^a Control Expert, all versions), PLC Simulator for EcoStruxure ^a Process Expert including all HDCS versions (former name of EcoStruxure ^a Process Expert, all versions), Modicon Quantum CPU (part numbers 140CPU*, all versions), Modicon Premium CPU (part numbers TSXP5*, all versions).		
NULL Pointer Dereference	02-Sep-21	5	A CWE-476: NULL Pointer Dereference vulnerability that could cause a Denial of Service on the Modicon PLC controller / simulator when updating the controller application with a specially crafted project file exists in Modicon M580 CPU (part numbers BMEP* and BMEH*, all versions), Modicon M340 CPU (part numbers BMXP34*, all versions), Modicon MC80 (part numbers BMKC80*, all	https://down load.schneide r- electric.com/f iles?p_Doc_Re f=SEVD- 2021-222-04	H-SCH-MODI- 170921/1930
CVSS Scoring Sc	ale 0-1	1-2	2-3 3-4 4-5 5-6	6-7 7-8	8-9 9-10

Page 682 of 1474

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			<pre>versions), Modicon Momentum Ethernet CPU (part numbers 171CBU*, all versions), PLC Simulator for EcoStruxure^a Control Expert, including all Unity Pro versions (former name of EcoStruxure^a Control Expert, all versions), PLC Simulator for EcoStruxure^a Process Expert including all HDCS versions (former name of EcoStruxure^a Process Expert, all versions), Modicon Quantum CPU (part numbers 140CPU*, all versions), Modicon Premium CPU (part numbers TSXP5*, all versions).</pre>		
modicon_m5	80_bmeh582	040s			
Improper Restriction of Operations within the Bounds of a Memory Buffer	02-Sep-21	4	A CWE-119: Improper Restriction of Operations within the Bounds of a Memory Buffer vulnerability that could cause a Denial of Service on the Modicon PLC controller / simulator when updating the controller application with a specially crafted project file exists in Modicon M580 CPU (part numbers BMEP* and BMEH*, all versions), Modicon M340 CPU (part numbers BMXP34*, all versions), Modicon MC80 (part numbers BMKC80*, all versions), Modicon	https://down load.schneide r- electric.com/f iles?p_Doc_Re f=SEVD- 2021-222-04	H-SCH-MODI- 170921/1931

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

Out-of- bounds Read 02-Sep-21 4 Momentum Ethernet CPU (part numbers 171CBU*, all versions), PLC Simulator for EcoStruxure ⁴ Control Expert, including all Unity Pro versions (former name of EcoStruxure ⁴ Process Expert including all HDCS versions), PLC Simulator for EcoStruxure ⁴ Process Expert including all HDCS versions), Modicon Quantum CPU (part numbers 140CPU*, all versions), Modicon Premium CPU (part numbers TSXP5*, all versions). CVE ID : CVE-2021-22789 A CWE-125: Out-of-bounds Read vulnerability that could cause a Denial of Service on the Modicon M580 CPU (part numbers BMEP* and BMEH*, all versions), Modicon M340 CPU (part numbers BMKP34*, all versions), Modicon Momentum Ethernet CPU (part numbers T37LGBU*, all versions), Modicon Momentum Ethernet CPU (part numbers T37LGBU*, all versions), Modicon Momentum Ethernet CPU (part numbers T37LGBU*, all versions), PLC Simulator for EcoStruxure ⁴ Control Expert, including all Unity Pro versions), PLC Simulator for EcoStruxure Control Expert, including all Unity Pro https://down	Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Out-of- bounds02-Sep-214Read vulnerability that could cause a Denial of Service on the Modicon PLC controller / simulator when updating the controller application with a specially crafted project file exists in Modicon M580 CPU (part numbers BMEP* and BMEH*, all versions),https://down load.schneide electric.com/f iles?p_Doc_Re versions), Modicon MC80 (part numbers BMKC80*, all versions), Modicon Momentum Ethernet CPU (part numbers 171CBU*, all versions), PLC Simulator for EcoStruxure ^a Control Expert, including all Unity ProH-SCH-MODI- 170921/1932				(part numbers 171CBU*, all versions), PLC Simulator for EcoStruxure ^a Control Expert, including all Unity Pro versions (former name of EcoStruxure ^a Control Expert, all versions), PLC Simulator for EcoStruxure ^a Process Expert including all HDCS versions (former name of EcoStruxure ^a Process Expert, all versions), Modicon Quantum CPU (part numbers 140CPU*, all versions), Modicon Premium CPU (part numbers TSXP5*, all versions).		
CVSS Scoring Scale 0-1 1-2 2-3 3-4 4-5 5-6 6-7 7-8 8-9 9-10	bounds	02-Sep-21	4	Read vulnerability that could cause a Denial of Service on the Modicon PLC controller / simulator when updating the controller application with a specially crafted project file exists in Modicon M580 CPU (part numbers BMEP* and BMEH*, all versions), Modicon M340 CPU (part numbers BMXP34*, all versions), Modicon MC80 (part numbers BMKC80*, all versions), Modicon Momentum Ethernet CPU (part numbers 171CBU*, all versions), PLC Simulator for EcoStruxure ^a Control Expert, including all Unity Pro versions (former name of	load.schneide r- electric.com/f iles?p_Doc_Re f=SEVD-	

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			EcoStruxure ^a Control Expert, all versions), PLC Simulator for EcoStruxure ^a Process Expert including all HDCS versions (former name of EcoStruxure ^a Process Expert, all versions), Modicon Quantum CPU (part numbers 140CPU*, all versions), Modicon Premium CPU (part numbers TSXP5*, all versions). CVE ID : CVE-2021-22790		
Out-of- bounds Write	02-Sep-21	4	A CWE-787: Out-of-bounds Write vulnerability that could cause a Denial of Service on the Modicon PLC controller / simulator when updating the controller application with a specially crafted project file exists in Modicon M580 CPU (part numbers BMEP* and BMEH*, all versions), Modicon M340 CPU (part numbers BMXP34*, all versions), Modicon MC80 (part numbers BMKC80*, all versions), Modicon Momentum Ethernet CPU (part numbers 171CBU*, all versions), PLC Simulator for EcoStruxure ^a Control Expert, including all Unity Pro versions (former name of EcoStruxure ^a Control Expert, all versions), PLC Simulator for EcoStruxure ^a Process Expert including all HDCS versions (former name of EcoStruxure ^a Process Expert,	https://down load.schneide r- electric.com/f iles?p_Doc_Re f=SEVD- 2021-222-04	H-SCH-MODI- 170921/1933
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 & CVE ID	Patch	NCIIPC ID
			all versions), Modicon Quantum CPU (part numbers 140CPU*, all versions), Modicon Premium CPU (part numbers TSXP5*, all versions). CVE ID : CVE-2021-22791		
NULL Pointer Dereference	02-Sep-21	5	A CWE-476: NULL Pointer Dereference vulnerability that could cause a Denial of Service on the Modicon PLC controller / simulator when updating the controller application with a specially crafted project file exists in Modicon M580 CPU (part numbers BMEP* and BMEH*, all versions), Modicon M340 CPU (part numbers BMXP34*, all versions), Modicon MC80 (part numbers BMKC80*, all versions), Modicon Momentum Ethernet CPU (part numbers 171CBU*, all versions), PLC Simulator for EcoStruxure ^a Control Expert, including all Unity Pro versions (former name of EcoStruxure ^a Control Expert, all versions), PLC Simulator for EcoStruxure ^a Process Expert including all HDCS versions (former name of EcoStruxure ^a Process Expert, all versions), Modicon Quantum CPU (part numbers 140CPU*, all versions), Modicon Premium CPU (part numbers TSXP5*, all	https://down load.schneide r- electric.com/f iles?p_Doc_Re f=SEVD- 2021-222-04	H-SCH-MODI- 170921/1934
CVSS Scoring Sc	cale 0-1	1-2	2-3 3-4 4-5 5-6	6-7 7-8	8-9 9-10

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID			
			versions).					
			CVE ID : CVE-2021-22792					
modicon_m580_bmeh584040								
Improper Restriction of Operations within the Bounds of a Memory Buffer	02-Sep-21	4	A CWE-119: Improper Restriction of Operations within the Bounds of a Memory Buffer vulnerability that could cause a Denial of Service on the Modicon PLC controller / simulator when updating the controller application with a specially crafted project file exists in Modicon M580 CPU (part numbers BMEP* and BMEH*, all versions), Modicon M340 CPU (part numbers BMXP34*, all versions), Modicon MC80 (part numbers BMKC80*, all versions), Modicon Momentum Ethernet CPU (part numbers 171CBU*, all versions), PLC Simulator for EcoStruxure ^a Control Expert, including all Unity Pro versions (former name of EcoStruxure ^a Control Expert, all versions), PLC Simulator for EcoStruxure ^a Process Expert including all HDCS versions (former name of EcoStruxure ^a Process Expert, all versions), Modicon Quantum CPU (part numbers 140CPU*, all versions), Modicon Premium CPU (part numbers TSXP5*, all versions).	https://down load.schneide r- electric.com/f iles?p_Doc_Re f=SEVD- 2021-222-04	H-SCH-MODI- 170921/1935			

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2021-22789		
Out-of- bounds Read	02-Sep-21	4	A CWE-125: Out-of-bounds Read vulnerability that could cause a Denial of Service on the Modicon PLC controller / simulator when updating the controller application with a specially crafted project file exists in Modicon M580 CPU (part numbers BMEP* and BMEH*, all versions), Modicon M340 CPU (part numbers BMXP34*, all versions), Modicon MC80 (part numbers BMKC80*, all versions), Modicon Momentum Ethernet CPU (part numbers 171CBU*, all versions), PLC Simulator for EcoStruxure ^a Control Expert, including all Unity Pro versions (former name of EcoStruxure ^a Control Expert, all versions), PLC Simulator for EcoStruxure ^a Process Expert including all HDCS versions (former name of EcoStruxure ^a Process Expert, all versions), Modicon Quantum CPU (part numbers 140CPU*, all versions), Modicon Premium CPU (part numbers TSXP5*, all versions). CVE ID : CVE-2021-22790	https://down load.schneide r- electric.com/f iles?p_Doc_Re f=SEVD- 2021-222-04	H-SCH-MODI- 170921/1936
Out-of- bounds Write	02-Sep-21	4	A CWE-787: Out-of-bounds Write vulnerability that could cause a Denial of Service on the Modicon PLC controller /	https://down load.schneide r- electric.com/f	H-SCH-MODI- 170921/1937

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
			simulator when updating the controller application with a specially crafted project file exists in Modicon M580 CPU (part numbers BMEP* and BMEH*, all versions), Modicon M340 CPU (part numbers BMXP34*, all versions), Modicon MC80 (part numbers BMKC80*, all versions), Modicon Momentum Ethernet CPU (part numbers 171CBU*, all versions), PLC Simulator for EcoStruxure ^a Control Expert, including all Unity Pro versions (former name of EcoStruxure ^a Control Expert, all versions), PLC Simulator for EcoStruxure ^a Process Expert including all HDCS versions (former name of EcoStruxure ^a Process Expert, all versions), Modicon Quantum CPU (part numbers 140CPU*, all versions), Modicon Premium CPU (part numbers TSXP5*, all versions).	iles?p_Doc_Re f=SEVD- 2021-222-04	
NULL Pointer Dereference CVSS Scoring Sc	02-Sep-21	5	A CWE-476: NULL Pointer Dereference vulnerability that could cause a Denial of Service on the Modicon PLC controller / simulator when updating the controller application with a specially crafted project file exists in Modicon M580 CPU (part numbers BMEP* and BMEH*, 2-3 3-4 4-5 5-6	https://down load.schneide r- electric.com/f iles?p_Doc_Re f=SEVD- 2021-222-04	H-SCH-MODI- 170921/1938 8-9 9-10

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			all versions), Modicon M340 CPU (part numbers BMXP34*, all versions), Modicon MC80 (part numbers BMKC80*, all versions), Modicon Momentum Ethernet CPU (part numbers 171CBU*, all versions), PLC Simulator for EcoStruxure ^a Control Expert, including all Unity Pro versions (former name of EcoStruxure ^a Control Expert, all versions), PLC Simulator for EcoStruxure ^a Process Expert including all HDCS versions (former name of EcoStruxure ^a Process Expert, all versions), Modicon Quantum CPU (part numbers 140CPU*, all versions), Modicon Premium CPU (part numbers TSXP5*, all versions). CVE ID : CVE-2021-22792		
modicon_m5	80 hmeh584	040c			
Improper Restriction of Operations within the Bounds of a Memory Buffer	02-Sep-21	4	A CWE-119: Improper Restriction of Operations within the Bounds of a Memory Buffer vulnerability that could cause a Denial of Service on the Modicon PLC controller / simulator when updating the controller application with a specially crafted project file exists in Modicon M580 CPU (part numbers BMEP* and BMEH*, all versions), Modicon M340	https://down load.schneide r- electric.com/f iles?p_Doc_Re f=SEVD- 2021-222-04	H-SCH-MODI- 170921/1939

CVSS Scoring Scale	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10
Dage 600 of 1474										

			CPU (part numbers BMXP34*, all versions), Modicon MC80 (part numbers BMKC80*, all versions), Modicon Momentum Ethernet CPU (part numbers 171CBU*, all versions), PLC Simulator for EcoStruxure ^a Control Expert, including all Unity Pro versions (former name of EcoStruxure ^a Control Expert, all versions), PLC Simulator for EcoStruxure ^a Process Expert including all HDCS versions (former name of EcoStruxure ^a Process Expert, all versions), Modicon Quantum CPU (part numbers 140CPU*, all versions), Modicon Premium CPU (part numbers TSXP5*, all versions). CVE ID : CVE-2021-22789		
Out-of- bounds Read	02-Sep-21	4	A CWE-125: Out-of-bounds Read vulnerability that could cause a Denial of Service on the Modicon PLC controller / simulator when updating the controller application with a specially crafted project file exists in Modicon M580 CPU (part numbers BMEP* and BMEH*, all versions), Modicon M340 CPU (part numbers BMXP34*, all versions), Modicon MC80 (part numbers BMKC80*, all versions), Modicon	https://down load.schneide r- electric.com/f iles?p_Doc_Re f=SEVD- 2021-222-04	H-SCH-MODI- 170921/1940

Out-of- bounds 02-Sep-21 4 (part numbers 171CBU*, all versions), PLC Simulator for EcoStruxure ^a Control Expert, all versions), PLC Simulator for EcoStruxure ^a Process Expert including all HDCS versions (former name of EcoStruxure ^a Process Expert, all versions), Modicon Quantum CPU (part numbers 140CPU*, all versions), Modicon Premium CPU (part numbers TSXP5*, all versions). • CVE ID : CVE-2021-22790 • A CWE-787: Out-of-bounds Write • 02-Sep-21 4 Modicon M580 CPU (part numbers BMEP* and BMEH*, all versions), Modicon M580 CPU (part numbers BMEP* and BMEH*, all versions), Modicon M580 CPU (part numbers BMK29*, all versions), Modicon M680 (part numbers MK209*, all	Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Out-of- bounds02-Sep-21ANeite vulnerability that could cause a Denial of Service on the Modicon PLC controller / simulator when updating the controller application with a specially crafted project file exists in Modicon M580 CPU (part numbers BMEP* and BMEH*, all versions), Nodicon M340 CPU (part lest), Modicon M340 CPU (part ersions), Modicon MC80 (part numbers BMXP34*, all versions), Modicon MC80 (part numbers BMKC80*, all) (part numbers 171CBU*, all) versions), PLC Simulator for EcoStruxure ^a Control Expert, including all Unity Pro versions (former name of EcoStruxure ^a Control Expert, including all Unity ProH-SCH-MODI- H-SCH-MODI- 10221-222-04				versions), PLC Simulator for EcoStruxure ^a Control Expert, including all Unity Pro versions (former name of EcoStruxure ^a Control Expert, all versions), PLC Simulator for EcoStruxure ^a Process Expert including all HDCS versions (former name of EcoStruxure ^a Process Expert, all versions), Modicon Quantum CPU (part numbers 140CPU*, all versions), Modicon Premium CPU (part numbers TSXP5*, all versions).		
	bounds Write		4	A CWE-787: Out-of-bounds Write vulnerability that could cause a Denial of Service on the Modicon PLC controller / simulator when updating the controller application with a specially crafted project file exists in Modicon M580 CPU (part numbers BMEP* and BMEH*, all versions), Modicon M340 CPU (part numbers BMXP34*, all versions), Modicon MC80 (part numbers BMKC80*, all versions), Modicon Momentum Ethernet CPU (part numbers 171CBU*, all versions), PLC Simulator for EcoStruxure ^a Control Expert, including all Unity Pro versions (former name of EcoStruxure ^a Control Expert,	load.schneide r- electric.com/f iles?p_Doc_Re f=SEVD- 2021-222-04	

Page 692 of 1474

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			all versions), PLC Simulator for EcoStruxure ^a Process Expert including all HDCS versions (former name of EcoStruxure ^a Process Expert, all versions), Modicon Quantum CPU (part numbers 140CPU*, all versions), Modicon Premium CPU (part numbers TSXP5*, all versions).		
			CVE ID : CVE-2021-22791		
NULL Pointer Dereference	02-Sep-21	5	A CWE-476: NULL Pointer Dereference vulnerability that could cause a Denial of Service on the Modicon PLC controller / simulator when updating the controller application with a specially crafted project file exists in Modicon M580 CPU (part numbers BMEP* and BMEH*, all versions), Modicon M340 CPU (part numbers BMXP34*, all versions), Modicon MC80 (part numbers BMKC80*, all versions), Modicon Momentum Ethernet CPU (part numbers 171CBU*, all versions), PLC Simulator for EcoStruxure ^a Control Expert, including all Unity Pro versions (former name of EcoStruxure ^a Control Expert, all versions), PLC Simulator for EcoStruxure ^a Process Expert including all HDCS versions (former name of EcoStruxure ^a Process Expert,	https://down load.schneide r- electric.com/f iles?p_Doc_Re f=SEVD- 2021-222-04	H-SCH-MODI- 170921/1942
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 & CVE ID	Patch	NCIIPC ID
			all versions), Modicon Quantum CPU (part numbers 140CPU*, all versions), Modicon Premium CPU (part numbers TSXP5*, all versions). CVE ID : CVE-2021-22792		
modicon_m5	580_bmeh584	040s			
Improper Restriction of Operations within the Bounds of a Memory Buffer	02-Sep-21	4	A CWE-119: Improper Restriction of Operations within the Bounds of a Memory Buffer vulnerability that could cause a Denial of Service on the Modicon PLC controller / simulator when updating the controller application with a specially crafted project file exists in Modicon M580 CPU (part numbers BMEP* and BMEH*, all versions), Modicon M340 CPU (part numbers BMXP34*, all versions), Modicon MC80 (part numbers BMKC80*, all versions), Modicon Momentum Ethernet CPU (part numbers 171CBU*, all versions), PLC Simulator for EcoStruxure ^a Control Expert, including all Unity Pro versions (former name of EcoStruxure ^a Control Expert, all versions), PLC Simulator for EcoStruxure ^a Process Expert including all HDCS versions (former name of EcoStruxure ^a Process Expert, all versions), Modicon	https://down load.schneide r- electric.com/f iles?p_Doc_Re f=SEVD- 2021-222-04	H-SCH-MODI- 170921/1943

CVSS Scoring Scale	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10
			D		f 1 / 7 /					

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Quantum CPU (part numbers 140CPU*, all versions), Modicon Premium CPU (part numbers TSXP5*, all versions). CVE ID : CVE-2021-22789		
Out-of- bounds Read	02-Sep-21	4	A CWE-125: Out-of-bounds Read vulnerability that could cause a Denial of Service on the Modicon PLC controller / simulator when updating the controller application with a specially crafted project file exists in Modicon M580 CPU (part numbers BMEP* and BMEH*, all versions), Modicon M340 CPU (part numbers BMXP34*, all versions), Modicon MC80 (part numbers BMKC80*, all versions), Modicon Momentum Ethernet CPU (part numbers 171CBU*, all versions), PLC Simulator for EcoStruxure ^a Control Expert, including all Unity Pro versions (former name of EcoStruxure ^a Control Expert, all versions), PLC Simulator for EcoStruxure ^a Process Expert including all HDCS versions (former name of EcoStruxure ^a Process Expert, all versions), Modicon Quantum CPU (part numbers 140CPU*, all versions), Modicon Premium CPU (part numbers TSXP5*, all versions).	https://down load.schneide r- electric.com/f iles?p_Doc_Re f=SEVD- 2021-222-04	H-SCH-MODI- 170921/1944

CVSS Scoring Scale	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10
			Pa	age 695 c	of 1474					

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2021-22790		
Out-of- bounds Write	02-Sep-21	4	A CWE-787: Out-of-bounds Write vulnerability that could cause a Denial of Service on the Modicon PLC controller / simulator when updating the controller application with a specially crafted project file exists in Modicon M580 CPU (part numbers BMEP* and BMEH*, all versions), Modicon M340 CPU (part numbers BMXP34*, all versions), Modicon MC80 (part numbers BMKC80*, all versions), Modicon Momentum Ethernet CPU (part numbers 171CBU*, all versions), PLC Simulator for EcoStruxure ^a Control Expert, including all Unity Pro versions (former name of EcoStruxure ^a Control Expert, all versions), PLC Simulator for EcoStruxure ^a Process Expert including all HDCS versions (former name of EcoStruxure ^a Process Expert, all versions), Modicon Quantum CPU (part numbers 140CPU*, all versions), Modicon Premium CPU (part numbers TSXP5*, all versions). CVE ID : CVE-2021-22791	https://down load.schneide r- electric.com/f iles?p_Doc_Re f=SEVD- 2021-222-04	H-SCH-MODI- 170921/1945
NULL Pointer Dereference	02-Sep-21	5	A CWE-476: NULL Pointer Dereference vulnerability that could cause a Denial of Service on the Modicon PLC	https://down load.schneide r- electric.com/f	H-SCH-MODI- 170921/1946

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

Page 696 of 1474

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			controller / simulator when updating the controller application with a specially crafted project file exists in Modicon M580 CPU (part numbers BMEP* and BMEH*, all versions), Modicon M340 CPU (part numbers BMXP34*, all versions), Modicon MC80 (part numbers BMKC80*, all versions), Modicon Momentum Ethernet CPU (part numbers 171CBU*, all versions), PLC Simulator for EcoStruxure ^a Control Expert, including all Unity Pro versions (former name of EcoStruxure ^a Control Expert, all versions), PLC Simulator for EcoStruxure ^a Process Expert including all HDCS versions (former name of EcoStruxure ^a Process Expert, all versions), Modicon Quantum CPU (part numbers 140CPU*, all versions), Modicon Premium CPU (part numbers TSXP5*, all versions).	iles?p_Doc_Re f=SEVD- 2021-222-04	
modicon_m5	80_bmeh586	040			
Improper Restriction of Operations within the Bounds of a Memory	02-Sep-21	4	A CWE-119: Improper Restriction of Operations within the Bounds of a Memory Buffer vulnerability that could cause a Denial of Service on the Modicon PLC controller / simulator when	https://down load.schneide r- electric.com/f iles?p_Doc_Re f=SEVD- 2021-222-04	H-SCH-MODI- 170921/1947
CVSS Scoring Sco	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
Buffer			updating the controller application with a specially crafted project file exists in Modicon M580 CPU (part numbers BMEP* and BMEH*, all versions), Modicon M340 CPU (part numbers BMXP34*, all versions), Modicon MC80 (part numbers BMKC80*, all versions), Modicon Momentum Ethernet CPU (part numbers 171CBU*, all versions), PLC Simulator for EcoStruxure ^a Control Expert, including all Unity Pro versions (former name of EcoStruxure ^a Control Expert, all versions), PLC Simulator for EcoStruxure ^a Process Expert including all HDCS versions (former name of EcoStruxure ^a Process Expert, all versions), Modicon Quantum CPU (part numbers 140CPU*, all versions), Modicon Premium CPU (part numbers TSXP5*, all versions).		
			CVE ID : CVE-2021-22789		
Out-of- bounds Read	02-Sep-21	4	A CWE-125: Out-of-bounds Read vulnerability that could cause a Denial of Service on the Modicon PLC controller / simulator when updating the controller application with a specially crafted project file exists in Modicon M580 CPU (part numbers BMEP* and BMEH*, all versions),	https://down load.schneide r- electric.com/f iles?p_Doc_Re f=SEVD- 2021-222-04	H-SCH-MODI- 170921/1948

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Modicon M340 CPU (part numbers BMXP34*, all versions), Modicon MC80 (part numbers BMKC80*, all versions), Modicon Momentum Ethernet CPU (part numbers 171CBU*, all versions), PLC Simulator for EcoStruxure ^a Control Expert, including all Unity Pro versions (former name of EcoStruxure ^a Control Expert, all versions), PLC Simulator for EcoStruxure ^a Process Expert including all HDCS versions (former name of EcoStruxure ^a Process Expert, all versions), Modicon Quantum CPU (part numbers 140CPU*, all versions), Modicon Premium CPU (part numbers TSXP5*, all versions).		
Out-of- bounds Write	02-Sep-21	4	A CWE-787: Out-of-bounds Write vulnerability that could cause a Denial of Service on the Modicon PLC controller / simulator when updating the controller application with a specially crafted project file exists in Modicon M580 CPU (part numbers BMEP* and BMEH*, all versions), Modicon M340 CPU (part numbers BMXP34*, all versions), Modicon MC80 (part numbers BMKC80*, all versions), Modicon	https://down load.schneide r- electric.com/f iles?p_Doc_Re f=SEVD- 2021-222-04	H-SCH-MODI- 170921/1949
CVSS Scoring Sc	ale 0-1	1-2	2-3 3-4 4-5 5-6	6-7 7-8	8-9 9-10

NULL Pointer Dereference02-Sep-2156ACWE-476: NULL Pointer pursions), PLC Simulator for EcoStruxure ^a Control Expert, all versions), PLC Simulator for EcoStruxure ^a Process Expert including all HDCS versions (former name of EcoStruxure ^a Process Expert, all versions), Modicon Quantum CPU (part numbers 140CPU*, all versions), Modicon Premium CPU (part numbers TSXP5*, all versions).Https://down load schneider r electric.com/f iles?p.Doc.Re for Service on the Modicon PLC controller / simulator moders application with a specially crafted project file exists in Modicon Modern MC80 (part numbers BMKC80*, all versions), Modiconhttps://down load schneider r electric.com/f iles?p.Doc.Re ferSEVD- 2021-222-04H-SCH-MODI- 170921/1950NULL Pointer Dereference02-Sep-215Service on the Modicon M340 CPU (part numbers bModicon M280 CPU (part numbers BMKC80*, all versions), Modicon M340 CPU (part numbers bMC800 part numbers BMKC80*, all versions), Modicon M340 CPU (part numbers 717CBU*, all versions), Modicon M340 cordical gall bury Pro versions (former name ofH-SCH-MODI- 170921/1950	Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
NULL Pointer Dereference02-Sep-215Dereference vulnerability that could cause a Denial of Service on the Modicon PLC controller / simulator when updating the controller application with a specially crafted project file exists in Modicon M580 CPU (part numbers BMEP* and BMEH*, all versions), Modicon M340 CPU (part numbers BMXP34*, all versions), Modicon MC80 (part numbers BMKC80*, all versions), Modicon Momentum Ethernet CPU (part numbers 171CBU*, all versions), PLC Simulator for EcoStruxureª Control Expert, including all Unity ProH-SCH-MODI- las?p_Doc_Re f=SEVD- 2021-222-04H-SCH-MODI- 170921/1950				versions), PLC Simulator for EcoStruxure ^a Control Expert, including all Unity Pro versions (former name of EcoStruxure ^a Control Expert, all versions), PLC Simulator for EcoStruxure ^a Process Expert including all HDCS versions (former name of EcoStruxure ^a Process Expert, all versions), Modicon Quantum CPU (part numbers 140CPU*, all versions), Modicon Premium CPU (part numbers TSXP5*, all versions).		
	Pointer	02-Sep-21	5	A CWE-476: NULL Pointer Dereference vulnerability that could cause a Denial of Service on the Modicon PLC controller / simulator when updating the controller application with a specially crafted project file exists in Modicon M580 CPU (part numbers BMEP* and BMEH*, all versions), Modicon M340 CPU (part numbers BMXP34*, all versions), Modicon MC80 (part numbers BMKC80*, all versions), Modicon Momentum Ethernet CPU (part numbers 171CBU*, all versions), PLC Simulator for EcoStruxure ^a Control Expert, including all Unity Pro	load.schneide r- electric.com/f iles?p_Doc_Re f=SEVD-	

Page 700 of 1474

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			EcoStruxure ^a Control Expert, all versions), PLC Simulator for EcoStruxure ^a Process Expert including all HDCS versions (former name of EcoStruxure ^a Process Expert, all versions), Modicon Quantum CPU (part numbers 140CPU*, all versions), Modicon Premium CPU (part numbers TSXP5*, all versions). CVE ID : CVE-2021-22792		
modicon_m5	80_bmeh586	040c			
Improper Restriction of Operations within the Bounds of a Memory Buffer	02-Sep-21	4	A CWE-119: Improper Restriction of Operations within the Bounds of a Memory Buffer vulnerability that could cause a Denial of Service on the Modicon PLC controller / simulator when updating the controller application with a specially crafted project file exists in Modicon M580 CPU (part numbers BMEP* and BMEH*, all versions), Modicon M340 CPU (part numbers BMXP34*, all versions), Modicon MC80 (part numbers BMKC80*, all versions), Modicon Momentum Ethernet CPU (part numbers 171CBU*, all versions), PLC Simulator for EcoStruxure ^a Control Expert, including all Unity Pro versions (former name of EcoStruxure ^a Control Expert,	https://down load.schneide r- electric.com/f iles?p_Doc_Re f=SEVD- 2021-222-04	H-SCH-MODI- 170921/1951

CVSS Scoring Scale	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10
			р	200 701 0	f 1 1 7 1					

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			all versions), PLC Simulator for EcoStruxure ^a Process Expert including all HDCS versions (former name of EcoStruxure ^a Process Expert, all versions), Modicon Quantum CPU (part numbers 140CPU*, all versions), Modicon Premium CPU (part numbers TSXP5*, all versions). CVE ID : CVE-2021-22789		
Out-of- bounds Read	02-Sep-21	4	A CWE-125: Out-of-bounds Read vulnerability that could cause a Denial of Service on the Modicon PLC controller / simulator when updating the controller application with a specially crafted project file exists in Modicon M580 CPU (part numbers BMEP* and BMEH*, all versions), Modicon M340 CPU (part numbers BMXP34*, all versions), Modicon MC80 (part numbers BMKC80*, all versions), Modicon Momentum Ethernet CPU (part numbers 171CBU*, all versions), PLC Simulator for EcoStruxure ^a Control Expert, including all Unity Pro versions (former name of EcoStruxure ^a Control Expert, all versions), PLC Simulator for EcoStruxure ^a Process Expert including all HDCS versions (former name of EcoStruxure ^a Process Expert, all versions), Modicon	https://down load.schneide r- electric.com/f iles?p_Doc_Re f=SEVD- 2021-222-04	H-SCH-MODI- 170921/1952

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Quantum CPU (part numbers 140CPU*, all versions), Modicon Premium CPU (part numbers TSXP5*, all versions). CVE ID : CVE-2021-22790		
Out-of- bounds Write	02-Sep-21	4	A CWE-787: Out-of-bounds Write vulnerability that could cause a Denial of Service on the Modicon PLC controller / simulator when updating the controller application with a specially crafted project file exists in Modicon M580 CPU (part numbers BMEP* and BMEH*, all versions), Modicon M340 CPU (part numbers BMXP34*, all versions), Modicon MC80 (part numbers BMKC80*, all versions), Modicon Momentum Ethernet CPU (part numbers 171CBU*, all versions), PLC Simulator for EcoStruxure ^a Control Expert, including all Unity Pro versions (former name of EcoStruxure ^a Control Expert, all versions), PLC Simulator for EcoStruxure ^a Process Expert including all HDCS versions (former name of EcoStruxure ^a Process Expert, all versions), Modicon Quantum CPU (part numbers 140CPU*, all versions), Modicon Premium CPU (part numbers TSXP5*, all versions).	https://down load.schneide r- electric.com/f iles?p_Doc_Re f=SEVD- 2021-222-04	H-SCH-MODI- 170921/1953

Γ	CVSS Scoring Scale	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10
Page 703 of 1474											

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2021-22791		
NULL Pointer Dereference	02-Sep-21	5	A CWE-476: NULL Pointer Dereference vulnerability that could cause a Denial of Service on the Modicon PLC controller / simulator when updating the controller application with a specially crafted project file exists in Modicon M580 CPU (part numbers BMEP* and BMEH*, all versions), Modicon M340 CPU (part numbers BMXP34*, all versions), Modicon MC80 (part numbers BMKC80*, all versions), Modicon Momentum Ethernet CPU (part numbers 171CBU*, all versions), PLC Simulator for EcoStruxure ^a Control Expert, including all Unity Pro versions (former name of EcoStruxure ^a Control Expert, all versions), PLC Simulator for EcoStruxure ^a Process Expert including all HDCS versions (former name of EcoStruxure ^a Process Expert, all versions), Modicon Quantum CPU (part numbers 140CPU*, all versions), Modicon Premium CPU (part numbers TSXP5*, all versions). CVE ID : CVE-2021-22792	https://down load.schneide r- electric.com/f iles?p_Doc_Re f=SEVD- 2021-222-04	H-SCH-MODI- 170921/1954
modicon_m5	80_bmeh586	040s			
Improper Restriction	02-Sep-21	4	A CWE-119: Improper Restriction of Operations	https://down load.schneide	H-SCH-MODI- 170921/1955
CVSS Scoring Sc	cale 0-1	1-2	2-3 3-4 4-5 5-6 Page 704 of 1474	6-7 7-8	8-9 <u>9-10</u>

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
of Operations within the Bounds of a Memory Buffer			<pre>within the Bounds of a Memory Buffer vulnerability that could cause a Denial of Service on the Modicon PLC controller / simulator when updating the controller application with a specially crafted project file exists in Modicon M580 CPU (part numbers BMEP* and BMEH*, all versions), Modicon M340 CPU (part numbers BMXP34*, all versions), Modicon MC80 (part numbers BMKC80*, all versions), Modicon Momentum Ethernet CPU (part numbers 171CBU*, all versions), PLC Simulator for EcoStruxure^a Control Expert, including all Unity Pro versions (former name of EcoStruxure^a Control Expert, all versions), PLC Simulator for EcoStruxure^a Process Expert including all HDCS versions (former name of EcoStruxure^a Process Expert, all versions), Modicon Quantum CPU (part numbers 140CPU*, all versions), Modicon Premium CPU (part numbers TSXP5*, all versions). CVE ID : CVE-2021-22789</pre>	r- electric.com/f iles?p_Doc_Re f=SEVD- 2021-222-04	
Out-of- bounds Read CVSS Scoring Sc	02-Sep-21	4	A CWE-125: Out-of-bounds Read vulnerability that could cause a Denial of Service on the Modicon PLC controller / simulator when updating the 2-3 3-4 4-5 5-6	https://down load.schneide r- electric.com/f iles?p_Doc_Re 6-7 7-8	H-SCH-MODI- 170921/1956 8-9 9-10

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			controller application with a specially crafted project file exists in Modicon M580 CPU (part numbers BMEP* and BMEH*, all versions), Modicon M340 CPU (part numbers BMXP34*, all versions), Modicon MC80 (part numbers BMKC80*, all versions), Modicon Momentum Ethernet CPU (part numbers 171CBU*, all versions), PLC Simulator for EcoStruxure ^a Control Expert, including all Unity Pro versions (former name of EcoStruxure ^a Control Expert, all versions), PLC Simulator for EcoStruxure ^a Process Expert including all HDCS versions (former name of EcoStruxure ^a Process Expert, all versions), Modicon Quantum CPU (part numbers 140CPU*, all versions), Modicon Premium CPU (part numbers TSXP5*, all versions).	f=SEVD- 2021-222-04	
Out-of- bounds Write	02-Sep-21	4	A CWE-787: Out-of-bounds Write vulnerability that could cause a Denial of Service on the Modicon PLC controller / simulator when updating the controller application with a specially crafted project file exists in Modicon M580 CPU (part numbers BMEP* and BMEH*, all versions), Modicon M340 CPU (part	https://down load.schneide r- electric.com/f iles?p_Doc_Re f=SEVD- 2021-222-04	H-SCH-MODI- 170921/1957

NULL			numbers BMXP34*, all versions), Modicon MC80 (part numbers BMKC80*, all versions), Modicon Momentum Ethernet CPU (part numbers 171CBU*, all versions), PLC Simulator for EcoStruxure ^a Control Expert, including all Unity Pro versions (former name of EcoStruxure ^a Control Expert, all versions), PLC Simulator		
NULL			for EcoStruxure ^a Process Expert including all HDCS versions (former name of EcoStruxure ^a Process Expert, all versions), Modicon Quantum CPU (part numbers 140CPU*, all versions), Modicon Premium CPU (part numbers TSXP5*, all versions). CVE ID : CVE-2021-22791		
Pointer 02-Sep Dereference	o-21 5	;	A CWE-476: NULL Pointer Dereference vulnerability that could cause a Denial of Service on the Modicon PLC controller / simulator when updating the controller application with a specially crafted project file exists in Modicon M580 CPU (part numbers BMEP* and BMEH*, all versions), Modicon M340 CPU (part numbers BMXP34*, all versions), Modicon MC80 (part numbers BMKC80*, all versions), Modicon	https://down load.schneide r- electric.com/f iles?p_Doc_Re f=SEVD- 2021-222-04	H-SCH-MODI- 170921/1958

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID				
			(part numbers 171CBU*, all versions), PLC Simulator for EcoStruxure ^a Control Expert, including all Unity Pro versions (former name of EcoStruxure ^a Control Expert, all versions), PLC Simulator for EcoStruxure ^a Process Expert including all HDCS versions (former name of EcoStruxure ^a Process Expert, all versions), Modicon Quantum CPU (part numbers 140CPU*, all versions), Modicon Premium CPU (part numbers TSXP5*, all versions). CVE ID : CVE-2021-22792						
modicon_m580_bmep581020									
Improper Restriction of Operations within the Bounds of a Memory Buffer	02-Sep-21	4	A CWE-119: Improper Restriction of Operations within the Bounds of a Memory Buffer vulnerability that could cause a Denial of Service on the Modicon PLC controller / simulator when updating the controller application with a specially crafted project file exists in Modicon M580 CPU (part numbers BMEP* and BMEH*, all versions), Modicon M340 CPU (part numbers BMXP34*, all versions), Modicon MC80 (part numbers BMKC80*, all versions), Modicon Momentum Ethernet CPU (part numbers 171CBU*, all	https://down load.schneide r- electric.com/f iles?p_Doc_Re f=SEVD- 2021-222-04	H-SCH-MODI- 170921/1959				

	CVSS Scoring Scale	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-1
Page 708 of 1474											

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			versions), PLC Simulator for EcoStruxure ^a Control Expert, including all Unity Pro versions (former name of EcoStruxure ^a Control Expert, all versions), PLC Simulator for EcoStruxure ^a Process Expert including all HDCS versions (former name of EcoStruxure ^a Process Expert, all versions), Modicon Quantum CPU (part numbers 140CPU*, all versions), Modicon Premium CPU (part numbers TSXP5*, all versions). CVE ID : CVE-2021-22789		
Out-of- bounds Read	02-Sep-21	4	A CWE-125: Out-of-bounds Read vulnerability that could cause a Denial of Service on the Modicon PLC controller / simulator when updating the controller application with a specially crafted project file exists in Modicon M580 CPU (part numbers BMEP* and BMEH*, all versions), Modicon M340 CPU (part numbers BMXP34*, all versions), Modicon MC80 (part numbers BMKC80*, all versions), Modicon Momentum Ethernet CPU (part numbers 171CBU*, all versions), PLC Simulator for EcoStruxure ^a Control Expert, including all Unity Pro versions (former name of EcoStruxure ^a Control Expert, all versions), PLC Simulator	https://down load.schneide r- electric.com/f iles?p_Doc_Re f=SEVD- 2021-222-04	H-SCH-MODI- 170921/1960

Out-of-bounds 02-Sep-21 4 A CWE-787: Out-of-bounds Write valuerability that could cause a Denial of Service on the Modicon M580 CPU (part numbers BMEP* and BMEH*, all versions), Modicon M580 CPU (part numbers BMEP* and BMEH*, all versions), Modicon M580 CPU (part numbers BMEP* and BMEH*, all versions), Modicon M580 CPU (part numbers BMEP* and BMEH*, all versions), Modicon M580 CPU (part numbers BMEP* and BMEH*, all versions), Modicon M580 CPU (part numbers BMEP* and BMEH*, all versions), Modicon M580 CPU (part numbers BMEP* and BMEH*, all versions), Modicon M580 CPU (part numbers BMEP* and BMEH*, all versions), Modicon M580 CPU (part numbers BMEP* and BMEH*, all versions), Modicon M580 CPU (part numbers BMEP* and BMEH*, all versions), Modicon M580 CPU (part numbers BMEP* and BMEH*, all versions), Modicon M580 CPU (part numbers BMEP* and BMEH*, all versions), Modicon M580 CPU (part numbers BMEP* and BMEH*, all versions), Modicon M580 CPU (part numbers BMEP* and BMEH*, all versions), Modicon M580 CPU (part numbers BMEP* and BMEH*, all versions), Modicon M20 CPU (part numbers BMEP* and BMEH*, all versions), Modicon M20 CPU (part numbers BMED*, all versions), Modicon M20 CPU (part numbers BMED*, all versions), Modicon M20 CPU (part numbers BMED*, all versions), Modicon M20 CPU (part numbers DMED*, all versions), PLC Simulator for EcoStruxure® Control Expert, all versions), PLC Simulator for FCoStruxure® Control Expert, all versions), PLC Simulator for EcoStruxure® Control Expert, all versions), Modicon Quantum CPU (part numbers H-SCH-MODI-170921/1961 CVSS Scorting Scale P1 12 23 34 45 56 67 78 89 90	Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Out-of- bounds02-Sep-214Write vulnerability that could cause a Denial of Service on the Modicon PLC controller / simulator when updating the controller application with a specially crafted project file exists in Modicon M580 CPU (part numbers BMEP* and BMEH*, all versions), Modicon M340 CPU (part numbers BMXP34*, all versions), Modicon MC80 (part numbers BMKC80*, all (part numbers BMKC80*, all (part numbers DMKC80*, all versions), Modiconhttps://down load.schneide (part numbers BMKC80*, all ies?p_Doc_Re (part numbers 171CBU*, all versions), PLC Simulator for EcoStruxure ^a Control Expert, all versions), PLC Simulator for EcoStruxure ^a Control Expert, all versions), PLC Simulator for for EcoStruxure ^a Process Expert including all HDCS versions (former name of EcoStruxure ^a Process Expert, all versions), ModiconH-SCH-MODI- 170921/1961				Expert including all HDCS versions (former name of EcoStruxure ^a Process Expert, all versions), Modicon Quantum CPU (part numbers 140CPU*, all versions), Modicon Premium CPU (part numbers TSXP5*, all versions).		
	bounds Write			Write vulnerability that could cause a Denial of Service on the Modicon PLC controller / simulator when updating the controller application with a specially crafted project file exists in Modicon M580 CPU (part numbers BMEP* and BMEH*, all versions), Modicon M340 CPU (part numbers BMXP34*, all versions), Modicon MC80 (part numbers BMKC80*, all versions), Modicon MC80 (part numbers BMKC80*, all versions), Modicon Momentum Ethernet CPU (part numbers 171CBU*, all versions), PLC Simulator for EcoStruxure ^a Control Expert, including all Unity Pro versions (former name of EcoStruxure ^a Control Expert, all versions), PLC Simulator for EcoStruxure ^a Process Expert including all HDCS versions (former name of EcoStruxure ^a Process Expert, all versions), Modicon Quantum CPU (part numbers	load.schneide r- electric.com/f iles?p_Doc_Re f=SEVD- 2021-222-04	170921/1961

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Weakness	Publish Date	CVSS	140CPU*, all versions), Modicon Premium CPU (part numbers TSXP5*, all versions). CVE ID : CVE-2021-22791 A CWE-476: NULL Pointer Dereference vulnerability that could cause a Denial of Service on the Modicon PLC controller / simulator when updating the controller application with a specially crafted project file exists in Modicon M580 CPU (part numbers BMEP* and BMEH*, all versions), Modicon M340 CPU (part numbers BMXP34*, all versions),	Patch	NCIIPC ID
NULL Pointer Dereference	02-Sep-21	5	CPU (part numbers	https://down load.schneide r- electric.com/f iles?p_Doc_Re f=SEVD- 2021-222-04	H-SCH-MODI- 170921/1962

	CVSS Scoring Scale	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10
Page 711 of 1474											

Improper of for poperations within the Bounds of a Memory Buffer vulnerability that could cause a Denial of Service on the Modicon PLC controller / simulator when updating the controller application with a specially crafted project file exists in Modicon MS40 CPU (part numbers BMEP* and BMEH*, all versions), Modicon M340 CPU (part numbers BMXP34*, all versions), Modicon MC80 (part numbers BMK284*, all versions), Modicon M540 CPU (part numbers BMK284*, all versions), Modicon M540 CPU (part numbers 171CBU*, all versions), PLC Simulator for EcoStruxure ^a Control Expert, all versions), PLC Simulator for EcoStruxure ^a Process Expert including all HDCS versions), Modicon Quantum CPU (part numbers 140CPU*, all versions), Modicon PLC H-SCH-MODI- 170921/1963 11 EcoStruxure ^a Process Expert including all HDCS versions), Modicon Quantum CPU (part numbers 140CPU*, all versions), Modicon PLC H-SCH-MODI- 12021-222-04
Improper Restriction of Operations within the Bounds of a Memory Buffer vulnerability that could cause a Denial of Service on the Modicon PLC controller / simulator when updating the controller application with a specially crafted project file exists in Modicon MS80 CPU (part numbers BMEP* and BMEH*, all versions), Modicon M340 CPU (part numbers BMXP34*, all versions), Modicon M340 (Put (part numbers BMK20*, all versions), Modicon MC80 (part numbers DMK20*, all versions), PLC Simulator for EcoStruxureª Control Expert, all versions), PLC Simulator for EcoStruxureª Process Expert including all Unity Pro versions, Modicon Quantum CPU (part numbers 140CPU*, all versions), Modicon Versions, Modicon Quantum CPU (part numbers 140CPU*, all versions), Modicon Versions), Modicon Versions, Modicon Modicon Premium CPU (part numbers 140CPU*, all versions), Modicon Versions, Modicon Ve
Improper Restriction of Operations within the Bounds of a Memory Buffer vulnerability biat could cause a Denial of Service on the Modicon PLC controller / simulator when updating the controller application with a specially crafted project file exists in Modicon M580 CPU (part numbers BMEP* and BMEH*, all versions), Modicon M340 CPU (part numbers BMXP34*, all versions), Modicon M260 (part numbers BMK280*, all versions), Modicon M240 (part numbers DMK280*, all versions), Modicon for EcoStruxureª Control Expert, all versions), PLC Simulator for EcoStruxureª Control Expert, all versions), Modicon 2021-222-04H-SCH-MODI- 170921/1963Improper Restriction of operations within the Bounds of a Memory Buffer++ </td
CVE ID : CVE-2021-22789

 3-4
 4-5
 5-6
 6-7

 Page 712 of 1474

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Out-of- bounds Read	02-Sep-21	4	A CWE-125: Out-of-bounds Read vulnerability that could cause a Denial of Service on the Modicon PLC controller / simulator when updating the controller application with a specially crafted project file exists in Modicon M580 CPU (part numbers BMEP* and BMEH*, all versions), Modicon M340 CPU (part numbers BMXP34*, all versions), Modicon MC80 (part numbers BMKC80*, all versions), Modicon MC80 (part numbers BMKC80*, all versions), Modicon Momentum Ethernet CPU (part numbers 171CBU*, all versions), PLC Simulator for EcoStruxure ^a Control Expert, including all Unity Pro versions (former name of EcoStruxure ^a Control Expert, all versions), PLC Simulator for EcoStruxure ^a Process Expert including all HDCS versions (former name of EcoStruxure ^a Process Expert, all versions), Modicon Quantum CPU (part numbers 140CPU*, all versions), Modicon Premium CPU (part numbers TSXP5*, all versions).	https://down load.schneide r- electric.com/f iles?p_Doc_Re f=SEVD- 2021-222-04	H-SCH-MODI- 170921/1964
Out-of- bounds Write	02-Sep-21	4	A CWE-787: Out-of-bounds Write vulnerability that could cause a Denial of Service on the Modicon PLC controller / simulator when updating the controller application with a	https://down load.schneide r- electric.com/f iles?p_Doc_Re f=SEVD-	H-SCH-MODI- 170921/1965

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			specially crafted project file exists in Modicon M580 CPU (part numbers BMEP* and BMEH*, all versions), Modicon M340 CPU (part numbers BMXP34*, all versions), Modicon MC80 (part numbers BMKC80*, all versions), Modicon Momentum Ethernet CPU (part numbers 171CBU*, all versions), PLC Simulator for EcoStruxure ^a Control Expert, including all Unity Pro versions (former name of EcoStruxure ^a Control Expert, all versions), PLC Simulator for EcoStruxure ^a Process Expert including all HDCS versions (former name of EcoStruxure ^a Process Expert, all versions), Modicon Quantum CPU (part numbers 140CPU*, all versions), Modicon Premium CPU (part numbers TSXP5*, all versions).	2021-222-04	
NULL Pointer Dereference	02-Sep-21	5	A CWE-476: NULL Pointer Dereference vulnerability that could cause a Denial of Service on the Modicon PLC controller / simulator when updating the controller application with a specially crafted project file exists in Modicon M580 CPU (part numbers BMEP* and BMEH*, all versions), Modicon M340 CPU (part numbers	https://down load.schneide r- electric.com/f iles?p_Doc_Re f=SEVD- 2021-222-04	H-SCH-MODI- 170921/1966
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 & CVE ID	Patch	NCIIPC ID
			BMXP34*, all versions), Modicon MC80 (part numbers BMKC80*, all versions), Modicon Momentum Ethernet CPU (part numbers 171CBU*, all versions), PLC Simulator for EcoStruxure ^a Control Expert, including all Unity Pro versions (former name of EcoStruxure ^a Control Expert, all versions), PLC Simulator for EcoStruxure ^a Process Expert including all HDCS versions (former name of EcoStruxure ^a Process Expert, all versions), Modicon Quantum CPU (part numbers 140CPU*, all versions), Modicon Premium CPU (part numbers TSXP5*, all versions). CVE ID : CVE-2021-22792		
modicon_m5	80_bmep582	020			
Improper Restriction of Operations within the Bounds of a Memory Buffer	02-Sep-21	4	A CWE-119: Improper Restriction of Operations within the Bounds of a Memory Buffer vulnerability that could cause a Denial of Service on the Modicon PLC controller / simulator when updating the controller application with a specially crafted project file exists in Modicon M580 CPU (part numbers BMEP* and BMEH*, all versions), Modicon M340 CPU (part numbers BMXP34*, all versions),	https://down load.schneide r- electric.com/f iles?p_Doc_Re f=SEVD- 2021-222-04	H-SCH-MODI- 170921/1967

CVSS Scoring Scale	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10
			P	age 715 c	of 1474					

			Modicon MC80 (part numbers BMKC80*, all versions), Modicon Momentum Ethernet CPU (part numbers 171CBU*, all versions), PLC Simulator for EcoStruxure ^a Control Expert, including all Unity Pro versions (former name of EcoStruxure ^a Control Expert, all versions), PLC Simulator for EcoStruxure ^a Process Expert including all HDCS versions (former name of EcoStruxure ^a Process Expert, all versions), Modicon Quantum CPU (part numbers 140CPU*, all versions), Modicon Premium CPU (part numbers TSXP5*, all versions).		
Out-of- bounds Read CVSS Scoring Sca	02-Sep-21	4	A CWE-125: Out-of-bounds Read vulnerability that could cause a Denial of Service on the Modicon PLC controller / simulator when updating the controller application with a specially crafted project file exists in Modicon M580 CPU (part numbers BMEP* and BMEH*, all versions), Modicon M340 CPU (part numbers BMXP34*, all versions), Modicon MC80 (part numbers BMKC80*, all versions), Modicon Momentum Ethernet CPU (part numbers 171CBU*, all versions), PLC Simulator for	https://down load.schneide r- electric.com/f iles?p_Doc_Re f=SEVD- 2021-222-04	H-SCH-MODI- 170921/1968

Page 716 of 1474

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			EcoStruxure ^ª Control Expert, including all Unity Pro versions (former name of EcoStruxure ^ª Control Expert, all versions), PLC Simulator for EcoStruxure ^ª Process Expert including all HDCS versions (former name of EcoStruxure ^ª Process Expert, all versions), Modicon Quantum CPU (part numbers 140CPU*, all versions), Modicon Premium CPU (part numbers TSXP5*, all versions). CVE ID : CVE-2021-22790		
Out-of- bounds Write	02-Sep-21	4	A CWE-787: Out-of-bounds Write vulnerability that could cause a Denial of Service on the Modicon PLC controller / simulator when updating the controller application with a specially crafted project file exists in Modicon M580 CPU (part numbers BMEP* and BMEH*, all versions), Modicon M340 CPU (part numbers BMXP34*, all versions), Modicon MC80 (part numbers BMKC80*, all versions), Modicon Momentum Ethernet CPU (part numbers 171CBU*, all versions), PLC Simulator for EcoStruxure ^a Control Expert, including all Unity Pro versions (former name of EcoStruxure ^a Control Expert, all versions), PLC Simulator for EcoStruxure ^a Process	https://down load.schneide r- electric.com/f iles?p_Doc_Re f=SEVD- 2021-222-04	H-SCH-MODI- 170921/1969

NULL 02-Sep-21 5 A CWE-476: NULL Pointer Dereference 02-Sep-21 5 A CWE-476: NULL Pointer Dereference https://down loadschneider numbers 171CBU*, all versions), Modicon Premium CPU (part numbers TSXP5*, all versions). https://down loadschneider application with a specially crafted project file exists in Modicon MS80 CPU (part numbers MKC80*, all versions), Modicon BMXP34*, all versions), Modicon Momentum Ethernet CPU (part numbers 171CBU*, all versions), PLC Simulator for EcoStruxure ⁸ Control Expert, all versions), PLC Simulator for EcoStruxure ⁸ Control Expert, all versions), PLC Simulator for EcoStruxure ⁸ Process Expert including all HDCS versions (former name of EcoStruxure ⁸ Process Expert, all versions), Modicon https://down load.schneide r- electric.com/files?p.Doc_Re f=SEVD- 2021-222-04	Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
NULL Pointer Dereference02-Sep-215Dereference vulnerability that could cause a Denial of Service on the Modicon PLC controller / simulator when updating the controller application with a specially crafted project file exists in Modicon M580 CPU (part numbers BMEP* and BMEH*, all versions), Modicon M340 CPU (part numbers BMXP34*, all versions), Modicon MC80 (part numbers BMKC80*, all versions), Modiconhttps://down load.schneide r- electric.com/f iles?p_Doc_Re f=SEVD- 2021-222-04H-SCH-MODI- 170921/1970NULL Pointer Dereference02-Sep-215Modicon M580 CPU (part numbers BMKC80*, all versions), Modiconhttps://down load.schneide r- electric.com/f iles?p_Doc_Re f=SEVD- 2021-222-04H-SCH-MODI- 170921/1970Intersection recostruxure* Control Expert, all versions), PLC Simulator for EcoStruxure* Control Expert, all versions), PLC Simulator for EcoStruxure* Control Expert, all versions), PLC Simulator for EcoStruxure* Process Expert including all HDCS versions (former name of EcoStruxure* Process Expert, all versions), ModiconH-SCH-MODI- 170921/1970				versions (former name of EcoStruxure ^a Process Expert, all versions), Modicon Quantum CPU (part numbers 140CPU*, all versions), Modicon Premium CPU (part numbers TSXP5*, all versions).		
CVSS Scoring Scale 0-1 1-2 2-3 3-4 4-5 5-6 6-7 7-8 8-9 9-10	Pointer Dereference			Dereference vulnerability that could cause a Denial of Service on the Modicon PLC controller / simulator when updating the controller application with a specially crafted project file exists in Modicon M580 CPU (part numbers BMEP* and BMEH*, all versions), Modicon M340 CPU (part numbers BMXP34*, all versions), Modicon MC80 (part numbers BMKC80*, all versions), Modicon Momentum Ethernet CPU (part numbers 171CBU*, all versions), PLC Simulator for EcoStruxure ^a Control Expert, including all Unity Pro versions (former name of EcoStruxure ^a Control Expert, all versions), PLC Simulator for EcoStruxure ^a Process Expert including all HDCS versions (former name of EcoStruxure ^a Process Expert, all versions), Modicon	load.schneide r- electric.com/f iles?p_Doc_Re f=SEVD- 2021-222-04	

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
modicon_m5	80_bmep582	020h	140CPU*, all versions), Modicon Premium CPU (part numbers TSXP5*, all versions). CVE ID : CVE-2021-22792		
Improper Restriction of Operations within the Bounds of a Memory Buffer	02-Sep-21	4	A CWE-119: Improper Restriction of Operations within the Bounds of a Memory Buffer vulnerability that could cause a Denial of Service on the Modicon PLC controller / simulator when updating the controller application with a specially crafted project file exists in Modicon M580 CPU (part numbers BMEP* and BMEH*, all versions), Modicon M340 CPU (part numbers BMXP34*, all versions), Modicon MC80 (part numbers BMKC80*, all versions), Modicon Momentum Ethernet CPU (part numbers 171CBU*, all versions), PLC Simulator for EcoStruxure ^a Control Expert, including all Unity Pro versions (former name of EcoStruxure ^a Control Expert, all versions), PLC Simulator for EcoStruxure ^a Process Expert including all HDCS versions (former name of EcoStruxure ^a Process Expert, all versions), Modicon Quantum CPU (part numbers 140CPU*, all versions),	https://down load.schneide r- electric.com/f iles?p_Doc_Re f=SEVD- 2021-222-04	H-SCH-MODI- 180921/1971

CV/SS Scoring Scolo	0.1	1 0	n n	2.4	4 F	ГС	67	70	0.0	0.10		
CVSS Scoring Scale	0-1	1-2	2-3	3-4	4-5	0-C	0-7	7-8	8-9	9-10		
	Page 710 of 1474											

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Weakness Out-of- bounds Read	Publish Date	CVSS	Modicon Premium CPU (part numbers TSXP5*, all versions). CVE ID : CVE-2021-22789 A CWE-125: Out-of-bounds Read vulnerability that could cause a Denial of Service on the Modicon PLC controller / simulator when updating the controller application with a specially crafted project file exists in Modicon M580 CPU (part numbers BMEP* and BMEH*, all versions), Modicon M340 CPU (part numbers BMXP34*, all versions), Modicon MC80 (part numbers BMKC80*, all versions), Modicon Momentum Ethernet CPU (part numbers 171CBU*, all versions), PLC Simulator for EcoStruxure ^a Control Expert, including all Unity Pro	Patch Patch	NCIIPC ID
			including all Unity Pro versions (former name of EcoStruxure ^a Control Expert, all versions), PLC Simulator for EcoStruxure ^a Process Expert including all HDCS versions (former name of EcoStruxure ^a Process Expert, all versions), Modicon Quantum CPU (part numbers 140CPU*, all versions), Modicon Premium CPU (part numbers TSXP5*, all versions). CVE ID : CVE-2021-22790		
Out-of-	02-Sep-21	4	A CWE-787: Out-of-bounds	https://down	H-SCH-MODI-

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
bounds Write			Write vulnerability that could cause a Denial of Service on the Modicon PLC controller / simulator when updating the controller application with a specially crafted project file exists in Modicon M580 CPU (part numbers BMEP* and BMEH*, all versions), Modicon M340 CPU (part numbers BMXP34*, all versions), Modicon MC80 (part numbers BMKC80*, all versions), Modicon Momentum Ethernet CPU (part numbers 171CBU*, all versions), PLC Simulator for EcoStruxure ^a Control Expert, including all Unity Pro versions (former name of EcoStruxure ^a Control Expert, all versions), PLC Simulator for EcoStruxure ^a Process Expert including all HDCS versions (former name of EcoStruxure ^a Process Expert, all versions), Modicon Quantum CPU (part numbers 140CPU*, all versions), Modicon Premium CPU (part numbers TSXP5*, all versions).	load.schneide r- electric.com/f iles?p_Doc_Re f=SEVD- 2021-222-04	180921/1973
NULL Pointer Dereference CVSS Scoring Sc	02-Sep-21 ale 0-1	5	A CWE-476: NULL Pointer Dereference vulnerability that could cause a Denial of Service on the Modicon PLC controller / simulator when updating the controller application with a specially 2-3 3-4 4-5 5-6	https://down load.schneide r- electric.com/f iles?p_Doc_Re f=SEVD-	H-SCH-MODI- 180921/1974 8-9 9-10

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			crafted project file exists in Modicon M580 CPU (part numbers BMEP* and BMEH*, all versions), Modicon M340 CPU (part numbers BMXP34*, all versions), Modicon MC80 (part numbers BMKC80*, all versions), Modicon Momentum Ethernet CPU (part numbers 171CBU*, all versions), PLC Simulator for EcoStruxure ^a Control Expert, including all Unity Pro versions (former name of EcoStruxure ^a Control Expert, all versions), PLC Simulator for EcoStruxure ^a Process Expert including all HDCS versions (former name of EcoStruxure ^a Process Expert, all versions), Modicon Quantum CPU (part numbers 140CPU*, all versions), Modicon Premium CPU (part numbers TSXP5*, all versions). CVE ID : CVE-2021-22792	2021-222-04	
modicon_m5	80_bmep582	040			
Improper Restriction of Operations within the Bounds of a Memory Buffer	02-Sep-21	4	A CWE-119: Improper Restriction of Operations within the Bounds of a Memory Buffer vulnerability that could cause a Denial of Service on the Modicon PLC controller / simulator when updating the controller application with a specially crafted project file exists in	https://down load.schneide r- electric.com/f iles?p_Doc_Re f=SEVD- 2021-222-04	H-SCH-MODI- 180921/1975

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

			Modicon M580 CPU (part numbers BMEP* and BMEH*, all versions), Modicon M340 CPU (part numbers BMXP34*, all versions), Modicon MC80 (part numbers BMKC80*, all versions), Modicon Momentum Ethernet CPU (part numbers 171CBU*, all versions), PLC Simulator for EcoStruxure ^a Control Expert,		
			including all Unity Pro versions (former name of EcoStruxure ^a Control Expert, all versions), PLC Simulator for EcoStruxure ^a Process Expert including all HDCS versions (former name of EcoStruxure ^a Process Expert, all versions), Modicon Quantum CPU (part numbers 140CPU*, all versions), Modicon Premium CPU (part numbers TSXP5*, all versions). CVE ID : CVE-2021-22789		
Out-of- bounds 02 Read	2-Sep-21	4	A CWE-125: Out-of-bounds Read vulnerability that could cause a Denial of Service on the Modicon PLC controller / simulator when updating the controller application with a specially crafted project file exists in Modicon M580 CPU (part numbers BMEP* and BMEH*, all versions), Modicon M340 CPU (part numbers BMXP34*, all versions), Modicon MC80	https://down load.schneide r- electric.com/f iles?p_Doc_Re f=SEVD- 2021-222-04	H-SCH-MODI- 180921/1976

bounds Write02-Sep-214BMEH*, all versions), Modicon M340 CPU (part numbers BMXP34*, all versions), Modicon MC80 (part numbers BMKC80*, all versions), Modicon Momentum Ethernet CPUelectric.com/f iles?p_Doc_Re f=SEVD- 2021-222-04180921/197	Weakness Publi	ish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Out-of- bounds02-Sep-214Write vulnerability that could cause a Denial of Service on the Modicon PLC controller / simulator when updating the controller application with a specially crafted project file (part numbers BMEP* and BMEH*, all versions), Modicon M340 CPU (part numbers BMXP34*, all versions), Modicon MC80 (part numbers BMKC80*, all versions), Modicon Momentum Ethernet CPUhttps://down https://down load.schneide r- electric.com/f iles?p_Doc_Re f=SEVD- 2021-222-04H-SCH-MODI 180921/197				versions), Modicon Momentum Ethernet CPU (part numbers 171CBU*, all versions), PLC Simulator for EcoStruxure ^a Control Expert, including all Unity Pro versions (former name of EcoStruxure ^a Control Expert, all versions), PLC Simulator for EcoStruxure ^a Process Expert including all HDCS versions (former name of EcoStruxure ^a Process Expert, all versions), Modicon Quantum CPU (part numbers 140CPU*, all versions), Modicon Premium CPU (part numbers TSXP5*, all versions).		
versions), PLC Simulator for EcoStruxure ^a Control Expert,	bounds 02-S	Sep-21	4	Write vulnerability that could cause a Denial of Service on the Modicon PLC controller / simulator when updating the controller application with a specially crafted project file exists in Modicon M580 CPU (part numbers BMEP* and BMEH*, all versions), Modicon M340 CPU (part numbers BMXP34*, all versions), Modicon MC80 (part numbers BMKC80*, all versions), Modicon Momentum Ethernet CPU (part numbers 171CBU*, all versions), PLC Simulator for	load.schneide r- electric.com/f iles?p_Doc_Re f=SEVD-	H-SCH-MODI- 180921/1977

Page 724 of 1474

Pointer 02-Sep-21 5 DMVD24* all usersions) electric com/f	Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
NULL Pointer Dereference02-Sep-215Dereference vulnerability that could cause a Denial of Service on the Modicon PLC controller / simulator when updating the controller application with a specially crafted project file exists in Modicon M580 CPU (part numbers BMEP* and BMEH*, all versions), Modicon M340https://down load.schneide r- electric.com/f 180921/1978NULL Pointer Dereference02-Sep-215BMXP34*, all versions), Modicon MC80 (part numbers BMKC80*, all versions), Modicon 2021-222-04H-SCH-MODI- 180921/1978Modicon MC80 (part numbers BMKC80*, all versions), Modicon Momentum Ethernet CPU (part numbers 171CBU*, all versions), PLC Simulator for EcoStruxureª Control Expert, including all Unity Pro versions (former name of EcoStruxureª Control Expert, all versions), PLC SimulatorH-SCH-MODI- 180921/1978				versions (former name of EcoStruxure ^a Control Expert, all versions), PLC Simulator for EcoStruxure ^a Process Expert including all HDCS versions (former name of EcoStruxure ^a Process Expert, all versions), Modicon Quantum CPU (part numbers 140CPU*, all versions), Modicon Premium CPU (part numbers TSXP5*, all versions).		
	Pointer	02-Sep-21	5	Dereference vulnerability that could cause a Denial of Service on the Modicon PLC controller / simulator when updating the controller application with a specially crafted project file exists in Modicon M580 CPU (part numbers BMEP* and BMEH*, all versions), Modicon M340 CPU (part numbers BMXP34*, all versions), Modicon MC80 (part numbers BMKC80*, all versions), Modicon Momentum Ethernet CPU (part numbers 171CBU*, all versions), PLC Simulator for EcoStruxure ^a Control Expert, including all Unity Pro versions (former name of EcoStruxure ^a Control Expert, all versions), PLC Simulator	load.schneide r- electric.com/f iles?p_Doc_Re f=SEVD-	H-SCH-MODI- 180921/1978

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Expert including all HDCS versions (former name of EcoStruxure ^a Process Expert, all versions), Modicon Quantum CPU (part numbers 140CPU*, all versions), Modicon Premium CPU (part numbers TSXP5*, all versions). CVE ID : CVE-2021-22792		
modicon_m5	80_bmep582	040h			
Improper Restriction of Operations within the Bounds of a Memory Buffer	02-Sep-21	4	A CWE-119: Improper Restriction of Operations within the Bounds of a Memory Buffer vulnerability that could cause a Denial of Service on the Modicon PLC controller / simulator when updating the controller application with a specially crafted project file exists in Modicon M580 CPU (part numbers BMEP* and BMEH*, all versions), Modicon M340 CPU (part numbers BMXP34*, all versions), Modicon MC80 (part numbers BMKC80*, all versions), Modicon Momentum Ethernet CPU (part numbers 171CBU*, all versions), PLC Simulator for EcoStruxure ^a Control Expert, including all Unity Pro versions (former name of EcoStruxure ^a Control Expert, all versions), PLC Simulator for EcoStruxure ^a Process Expert including all HDCS	https://down load.schneide r- electric.com/f iles?p_Doc_Re f=SEVD- 2021-222-04	H-SCH-MODI- 180921/1979

	CVSS Scoring Scale	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10
Dago 726 of 1474											

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			versions (former name of EcoStruxure ^a Process Expert, all versions), Modicon Quantum CPU (part numbers 140CPU*, all versions), Modicon Premium CPU (part numbers TSXP5*, all versions). CVE ID : CVE-2021-22789		
Out-of- bounds Read	02-Sep-21	4	A CWE-125: Out-of-bounds Read vulnerability that could cause a Denial of Service on the Modicon PLC controller / simulator when updating the controller application with a specially crafted project file exists in Modicon M580 CPU (part numbers BMEP* and BMEH*, all versions), Modicon M340 CPU (part numbers BMXP34*, all versions), Modicon MC80 (part numbers BMKC80*, all versions), Modicon MC80 (part numbers BMKC80*, all versions), Modicon Momentum Ethernet CPU (part numbers 171CBU*, all versions), PLC Simulator for EcoStruxure ^a Control Expert, including all Unity Pro versions (former name of EcoStruxure ^a Control Expert, all versions), PLC Simulator for EcoStruxure ^a Process Expert including all HDCS versions (former name of EcoStruxure ^a Process Expert, all versions), Modicon Quantum CPU (part numbers 140CPU*, all versions), Modicon Premium CPU (part	https://down load.schneide r- electric.com/f iles?p_Doc_Re f=SEVD- 2021-222-04	H-SCH-MODI- 180921/1980
CVSS Scoring So	cale 0-1	1-2	2-3 3-4 4-5 5-6 Page 727 of 1474	6-7 7-8	8-9 <mark>9-10</mark>

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			numbers TSXP5*, all versions). CVE ID : CVE-2021-22790		
Out-of- bounds Write	02-Sep-21	4	A CWE-787: Out-of-bounds Write vulnerability that could cause a Denial of Service on the Modicon PLC controller / simulator when updating the controller application with a specially crafted project file exists in Modicon M580 CPU (part numbers BMEP* and BMEH*, all versions), Modicon M340 CPU (part numbers BMXP34*, all versions), Modicon MC80 (part numbers BMKC80*, all versions), Modicon MC80 (part numbers 171CBU*, all versions), PLC Simulator for EcoStruxure ^a Control Expert, including all Unity Pro versions (former name of EcoStruxure ^a Control Expert, all versions), PLC Simulator for EcoStruxure ^a Process Expert including all HDCS versions (former name of EcoStruxure ^a Process Expert, all versions), Modicon Quantum CPU (part numbers 140CPU*, all versions), Modicon Premium CPU (part numbers TSXP5*, all versions).	https://down load.schneide r- electric.com/f iles?p_Doc_Re f=SEVD- 2021-222-04	H-SCH-MODI- 180921/1981
NULL Pointer	02-Sep-21	5	A CWE-476: NULL Pointer Dereference vulnerability	https://down load.schneide	H-SCH-MODI- 180921/1982

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Dereference			that could cause a Denial of	r-	
			Service on the Modicon PLC	electric.com/f	
			controller / simulator when	iles?p_Doc_Re	
			updating the controller	f=SEVD-	
			application with a specially	2021-222-04	
			crafted project file exists in		
			Modicon M580 CPU (part		
			numbers BMEP* and BMEH*,		
			all versions), Modicon M340		
			CPU (part numbers		
			BMXP34*, all versions),		
			Modicon MC80 (part		
			numbers BMKC80*, all		
			versions), Modicon		
			Momentum Ethernet CPU		
			(part numbers 171CBU*, all		
			versions), PLC Simulator for		
			EcoStruxure ^a Control Expert,		
			including all Unity Pro		
			versions (former name of		
			EcoStruxure ^a Control Expert,		
			all versions), PLC Simulator		
			for EcoStruxure ^a Process		
			Expert including all HDCS		
			versions (former name of		
			EcoStruxure ^a Process Expert,		
			all versions), Modicon		
			Quantum CPU (part numbers		
			140CPU*, all versions),		
			Modicon Premium CPU (part		
			numbers TSXP5*, all		
			versions).		
			CVE ID : CVE-2021-22792		
modicon_m5	80 hmen582	040s			
	50_5mcp502	0103			
Improper			A CWE-119: Improper	https://down	
Restriction	02 San 21	4	Restriction of Operations	load.schneide	H-SCH-MODI-
of	02-Sep-21	4	within the Bounds of a	r-	180921/1983
Operations			Memory Buffer vulnerability	electric.com/f	-
within the			that could cause a Denial of	iles?p_Doc_Re	

CVSS Scoring Scale	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	
			Pa	age 729 o	of 1474				

8-9

9-10

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Bounds of a Memory Buffer			Service on the Modicon PLC controller / simulator when updating the controller application with a specially crafted project file exists in Modicon M580 CPU (part numbers BMEP* and BMEH*, all versions), Modicon M340 CPU (part numbers BMXP34*, all versions), Modicon MC80 (part numbers BMKC80*, all versions), Modicon Momentum Ethernet CPU (part numbers 171CBU*, all versions), PLC Simulator for EcoStruxure ^a Control Expert, including all Unity Pro versions (former name of EcoStruxure ^a Control Expert, all versions), PLC Simulator for EcoStruxure ^a Process Expert including all HDCS versions (former name of EcoStruxure ^a Process Expert, all versions), Modicon Quantum CPU (part numbers 140CPU*, all versions), Modicon Premium CPU (part numbers TSXP5*, all versions).	f=SEVD- 2021-222-04	
Out-of- bounds Read	02-Sep-21	4	A CWE-125: Out-of-bounds Read vulnerability that could cause a Denial of Service on the Modicon PLC controller / simulator when updating the controller application with a specially crafted project file exists in Modicon M580 CPU	https://down load.schneide r- electric.com/f iles?p_Doc_Re f=SEVD- 2021-222-04	H-SCH-MODI- 180921/1984

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			(part numbers BMEP* and BMEH*, all versions), Modicon M340 CPU (part numbers BMXP34*, all versions), Modicon MC80 (part numbers BMKC80*, all versions), Modicon Momentum Ethernet CPU (part numbers 171CBU*, all versions), PLC Simulator for EcoStruxure ^a Control Expert, including all Unity Pro versions (former name of EcoStruxure ^a Control Expert, all versions), PLC Simulator for EcoStruxure ^a Process Expert including all HDCS versions (former name of EcoStruxure ^a Process Expert, all versions), Modicon Quantum CPU (part numbers 140CPU*, all versions), Modicon Premium CPU (part numbers TSXP5*, all versions).		
Out-of- bounds Write	02-Sep-21	4	A CWE-787: Out-of-bounds Write vulnerability that could cause a Denial of Service on the Modicon PLC controller / simulator when updating the controller application with a specially crafted project file exists in Modicon M580 CPU (part numbers BMEP* and BMEH*, all versions), Modicon M340 CPU (part numbers BMXP34*, all versions), Modicon MC80 (part numbers BMKC80*, all	https://down load.schneide r- electric.com/f iles?p_Doc_Re f=SEVD- 2021-222-04	H-SCH-MODI- 180921/1985
CVSS Scoring Sc	ale 0-1	1-2	2-3 3-4 4-5 5-6	6-7 7-8	8-9 9-10

			versions), Modicon Momentum Ethernet CPU (part numbers 171CBU*, all versions), PLC Simulator for EcoStruxure ^a Control Expert, including all Unity Pro versions (former name of EcoStruxure ^a Control Expert, all versions), PLC Simulator for EcoStruxure ^a Process Expert including all HDCS versions (former name of EcoStruxure ^a Process Expert, all versions), Modicon Quantum CPU (part numbers 140CPU*, all versions), Modicon Premium CPU (part numbers TSXP5*, all versions).		
NULL Pointer Dereference	02-Sep-21	5	A CWE-476: NULL Pointer Dereference vulnerability that could cause a Denial of Service on the Modicon PLC controller / simulator when updating the controller application with a specially crafted project file exists in Modicon M580 CPU (part numbers BMEP* and BMEH*, all versions), Modicon M340 CPU (part numbers BMXP34*, all versions), Modicon MC80 (part numbers BMKC80*, all versions), Modicon Momentum Ethernet CPU (part numbers 171CBU*, all versions), PLC Simulator for EcoStruxure ^a Control Expert,	https://down load.schneide r- electric.com/f iles?p_Doc_Re f=SEVD- 2021-222-04	H-SCH-MODI- 180921/1986

Page 732 of 1474

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			including all Unity Pro versions (former name of EcoStruxure ^a Control Expert, all versions), PLC Simulator for EcoStruxure ^a Process Expert including all HDCS versions (former name of EcoStruxure ^a Process Expert, all versions), Modicon Quantum CPU (part numbers 140CPU*, all versions), Modicon Premium CPU (part numbers TSXP5*, all versions). CVE ID : CVE-2021-22792		
modicon_m5	80_bmep583	020			
Improper Restriction of Operations within the Bounds of a Memory Buffer	02-Sep-21	4	A CWE-119: Improper Restriction of Operations within the Bounds of a Memory Buffer vulnerability that could cause a Denial of Service on the Modicon PLC controller / simulator when updating the controller application with a specially crafted project file exists in Modicon M580 CPU (part numbers BMEP* and BMEH*, all versions), Modicon M340 CPU (part numbers BMXP34*, all versions), Modicon MC80 (part numbers BMKC80*, all versions), Modicon Momentum Ethernet CPU (part numbers 171CBU*, all versions), PLC Simulator for EcoStruxure ^a Control Expert, including all Unity Pro	https://down load.schneide r- electric.com/f iles?p_Doc_Re f=SEVD- 2021-222-04	H-SCH-MODI- 180921/1987

CVSS Scoring Scale	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10
			D	200 722 0	f 1/7/					

Out-of- bounds 02-Sep-2 Read	/eakness Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
bounds 02-Sep-2			versions (former name of EcoStruxure ^a Control Expert, all versions), PLC Simulator for EcoStruxure ^a Process Expert including all HDCS versions (former name of EcoStruxure ^a Process Expert, all versions), Modicon Quantum CPU (part numbers 140CPU*, all versions), Modicon Premium CPU (part numbers TSXP5*, all versions). CVE ID : CVE-2021-22789		
	inds 02-Sep-21	4	A CWE-125: Out-of-bounds Read vulnerability that could cause a Denial of Service on the Modicon PLC controller / simulator when updating the controller application with a specially crafted project file exists in Modicon M580 CPU (part numbers BMEP* and BMEH*, all versions), Modicon M340 CPU (part numbers BMXP34*, all versions), Modicon MC80 (part numbers BMKC80*, all versions), Modicon Momentum Ethernet CPU (part numbers 171CBU*, all versions), PLC Simulator for EcoStruxure ^a Control Expert, including all Unity Pro versions (former name of EcoStruxure ^a Control Expert, all versions), PLC Simulator for EcoStruxure ^a Process Expert including all HDCS versions (former name of	https://down load.schneide r- electric.com/f iles?p_Doc_Re f=SEVD- 2021-222-04	H-SCH-MODI- 180921/1988

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			EcoStruxure ^a Process Expert, all versions), Modicon Quantum CPU (part numbers 140CPU*, all versions), Modicon Premium CPU (part numbers TSXP5*, all versions). CVE ID : CVE-2021-22790		
Out-of- bounds Write	02-Sep-21	4	A CWE-787: Out-of-bounds Write vulnerability that could cause a Denial of Service on the Modicon PLC controller / simulator when updating the controller application with a specially crafted project file exists in Modicon M580 CPU (part numbers BMEP* and BMEH*, all versions), Modicon M340 CPU (part numbers BMXP34*, all versions), Modicon MC80 (part numbers BMKC80*, all versions), Modicon MC80 (part numbers BMKC80*, all versions), Modicon Momentum Ethernet CPU (part numbers 171CBU*, all versions), PLC Simulator for EcoStruxure ^a Control Expert, including all Unity Pro versions (former name of EcoStruxure ^a Control Expert, all versions), PLC Simulator for EcoStruxure ^a Process Expert including all HDCS versions (former name of EcoStruxure ^a Process Expert, all versions), Modicon Quantum CPU (part numbers 140CPU*, all versions), Modicon Premium CPU (part numbers TSXP5*, all	https://down load.schneide r- electric.com/f iles?p_Doc_Re f=SEVD- 2021-222-04	H-SCH-MODI- 180921/1989
CVSS Scoring Sc	cale 0-1	1-2	2-3 3-4 4-5 5-6	6-7 7-8	8-9 9-10

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			versions).		
			CVE ID : CVE-2021-22791		
NULL Pointer Dereference	02-Sep-21	5	A CWE-476: NULL Pointer Dereference vulnerability that could cause a Denial of Service on the Modicon PLC controller / simulator when updating the controller application with a specially crafted project file exists in Modicon M580 CPU (part numbers BMEP* and BMEH*, all versions), Modicon M340 CPU (part numbers BMXP34*, all versions), Modicon MC80 (part numbers BMKC80*, all versions), Modicon Momentum Ethernet CPU (part numbers 171CBU*, all versions), PLC Simulator for EcoStruxure ^a Control Expert, including all Unity Pro versions (former name of EcoStruxure ^a Control Expert, all versions), PLC Simulator for EcoStruxure ^a Process Expert including all HDCS versions (former name of EcoStruxure ^a Process Expert, all versions), Modicon Quantum CPU (part numbers 140CPU*, all versions), Modicon Premium CPU (part numbers TSXP5*, all versions). CVE ID : CVE-2021-22792	https://down load.schneide r- electric.com/f iles?p_Doc_Re f=SEVD- 2021-222-04	H-SCH-MODI- 180921/1990

CVSS Scoring Scale	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10
			Р	200 726 0	f 1 / 7 /					

Improper Restriction of Operations within the Bounds of a Memory Buffer vulnerability that could cause a Denial of Service on the Modicon PLC controller / simulator when updating the controller application with a specially crafted project file exists in Modicon M580 CPU (part numbers BMEP* and BMEH*, all versions), Modicon M580 CPU (part numbers BME2*and BMEH*, all versions), Modicon M580 CPU (part numbers BMK28*, all versions), Modicon M580 CPU (part numbers BMXP34*, all versions), Modicon M580 CPU (part numbers BMXP34*, all versions), Modicon M580 CPU (part numbers BMXP34*, all versions), Modicon M580 CPU (part numbers BMXP34*, all versions), Modicon M580 CPU (part numbers BMKC80*, all versions), PLC Simulator for EcoStruxure ^a Control Expert, all versions), PLC Simulator for EcoStruxure ^a Control Expert, all versions), PLC Simulator for EcoStruxure ^a Control Expert, all versions), Modicon Quantum CPU (part numbers 140CPI*, all versions), Modicon Pure versions (former name of EcoStruxure ^a Process Expert including all HDCS versions (former name of EcoStruxure ^a Process Expert including all HDCS versions), Modicon Quantum CPU (part numbers 140CPI*, all versions), Modicon Puremine CPU (part numbers TSXP5*, all versions). CVEID : CVE-2021-22789https://down load.schneide r-Out-of- bounds02-Sep-214AcWE-125: Out-of-bounds Read vulnerability that could case a Denial of Service on load.schneide r-https://down load.schneide r-	Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Out-of- 02-Sep-21 4 Read vulnerability that could load.schneide H-SCH-MODI- bounds 180921/1992	Restriction of Operations within the Bounds of a Memory	02-Sep-21	4	Restriction of Operations within the Bounds of a Memory Buffer vulnerability that could cause a Denial of Service on the Modicon PLC controller / simulator when updating the controller application with a specially crafted project file exists in Modicon M580 CPU (part numbers BMEP* and BMEH*, all versions), Modicon M340 CPU (part numbers BMXP34*, all versions), Modicon MC80 (part numbers BMKC80*, all versions), Modicon Momentum Ethernet CPU (part numbers 171CBU*, all versions), PLC Simulator for EcoStruxure ^a Control Expert, including all Unity Pro versions (former name of EcoStruxure ^a Control Expert, all versions), PLC Simulator for EcoStruxure ^a Process Expert including all HDCS versions (former name of EcoStruxure ^a Process Expert, all versions), Modicon Quantum CPU (part numbers 140CPU*, all versions), Modicon Premium CPU (part numbers TSXP5*, all versions).	load.schneide r- electric.com/f iles?p_Doc_Re f=SEVD-	
		02-Sep-21	4	Read vulnerability that could	load.schneide	

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Read			the Modicon PLC controller / simulator when updating the controller application with a specially crafted project file exists in Modicon M580 CPU (part numbers BMEP* and BMEH*, all versions), Modicon M340 CPU (part numbers BMXP34*, all versions), Modicon MC80 (part numbers BMKC80*, all versions), Modicon MC80 (part numbers BMKC80*, all versions), Modicon Momentum Ethernet CPU (part numbers 171CBU*, all versions), PLC Simulator for EcoStruxure ^a Control Expert, including all Unity Pro versions (former name of EcoStruxure ^a Control Expert, all versions), PLC Simulator for EcoStruxure ^a Process Expert including all HDCS versions (former name of EcoStruxure ^a Process Expert, all versions), Modicon Quantum CPU (part numbers 140CPU*, all versions), Modicon Premium CPU (part numbers TSXP5*, all versions).	electric.com/f iles?p_Doc_Re f=SEVD- 2021-222-04	
Out-of- bounds Write CVSS Scoring Sc	02-Sep-21	4	A CWE-787: Out-of-bounds Write vulnerability that could cause a Denial of Service on the Modicon PLC controller / simulator when updating the controller application with a specially crafted project file exists in Modicon M580 CPU (part numbers BMEP* and 2-3 3-4 4-5 5-6	https://down load.schneide r- electric.com/f iles?p_Doc_Re f=SEVD- 2021-222-04	H-SCH-MODI- 180921/1993 8-9 9-10

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			BMEH*, all versions), Modicon M340 CPU (part numbers BMXP34*, all versions), Modicon MC80 (part numbers BMKC80*, all versions), Modicon Momentum Ethernet CPU (part numbers 171CBU*, all versions), PLC Simulator for EcoStruxure ^a Control Expert, including all Unity Pro versions (former name of EcoStruxure ^a Control Expert, all versions), PLC Simulator for EcoStruxure ^a Process Expert including all HDCS versions (former name of EcoStruxure ^a Process Expert, all versions), Modicon Quantum CPU (part numbers 140CPU*, all versions), Modicon Premium CPU (part numbers TSXP5*, all versions).		
NULL Pointer Dereference	02-Sep-21	5	A CWE-476: NULL Pointer Dereference vulnerability that could cause a Denial of Service on the Modicon PLC controller / simulator when updating the controller application with a specially crafted project file exists in Modicon M580 CPU (part numbers BMEP* and BMEH*, all versions), Modicon M340 CPU (part numbers BMXP34*, all versions), Modicon MC80 (part numbers BMKC80*, all	https://down load.schneide r- electric.com/f iles?p_Doc_Re f=SEVD- 2021-222-04	H-SCH-MODI- 180921/1994
CVSS Scoring Sc	ale 0-1	1-2	2-3 3-4 4-5 5-6	6-7 7-8	8-9 9-10

Page 739 of 1474

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			<pre>versions), Modicon Momentum Ethernet CPU (part numbers 171CBU*, all versions), PLC Simulator for EcoStruxure^a Control Expert, including all Unity Pro versions (former name of EcoStruxure^a Control Expert, all versions), PLC Simulator for EcoStruxure^a Process Expert including all HDCS versions (former name of EcoStruxure^a Process Expert, all versions), Modicon Quantum CPU (part numbers 140CPU*, all versions), Modicon Premium CPU (part numbers TSXP5*, all versions).</pre>		
modicon_m5	80_bmep584	020			
Improper Restriction of Operations within the Bounds of a Memory Buffer	02-Sep-21	4	A CWE-119: Improper Restriction of Operations within the Bounds of a Memory Buffer vulnerability that could cause a Denial of Service on the Modicon PLC controller / simulator when updating the controller application with a specially crafted project file exists in Modicon M580 CPU (part numbers BMEP* and BMEH*, all versions), Modicon M340 CPU (part numbers BMXP34*, all versions), Modicon MC80 (part numbers BMKC80*, all versions), Modicon	https://down load.schneide r- electric.com/f iles?p_Doc_Re f=SEVD- 2021-222-04	H-SCH-MODI- 180921/1995

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

Out-of- bounds 02-Sep-21 4 Out-of- bounds 02-Sep-21 4 Out-of- bounds 02-Sep-21 4 Out-of- bounds 02-Sep-21 4	Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Out-of- bounds02-Sep-214Read vulnerability that could cause a Denial of Service on the Modicon PLC controller / simulator when updating the controller application with a specially crafted project file exists in Modicon M580 CPU (part numbers BMEP* and BMEH*, all versions),https://down load.schneide BMEH*, all versions),H-SCH-MODI- 180921/1996Read02-Sep-214Modicon M340 CPU (part 				(part numbers 171CBU*, all versions), PLC Simulator for EcoStruxure ^a Control Expert, including all Unity Pro versions (former name of EcoStruxure ^a Control Expert, all versions), PLC Simulator for EcoStruxure ^a Process Expert including all HDCS versions (former name of EcoStruxure ^a Process Expert, all versions), Modicon Quantum CPU (part numbers 140CPU*, all versions), Modicon Premium CPU (part numbers TSXP5*, all versions).		
CVSS Scoring Scale 0-1 1-2 2-3 3-4 4-5 5-6 6-7 7-8 8-9 9-10	bounds Read			Read vulnerability that could cause a Denial of Service on the Modicon PLC controller / simulator when updating the controller application with a specially crafted project file exists in Modicon M580 CPU (part numbers BMEP* and BMEH*, all versions), Modicon M340 CPU (part numbers BMXP34*, all versions), Modicon MC80 (part numbers BMKC80*, all versions), Modicon Momentum Ethernet CPU (part numbers 171CBU*, all versions), PLC Simulator for EcoStruxure ^a Control Expert, including all Unity Pro versions (former name of	load.schneide r- electric.com/f iles?p_Doc_Re f=SEVD- 2021-222-04	180921/1996

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			EcoStruxure ^a Control Expert, all versions), PLC Simulator for EcoStruxure ^a Process Expert including all HDCS versions (former name of EcoStruxure ^a Process Expert, all versions), Modicon Quantum CPU (part numbers 140CPU*, all versions), Modicon Premium CPU (part numbers TSXP5*, all versions). CVE ID : CVE-2021-22790		
Out-of- bounds Write	02-Sep-21	4	A CWE-787: Out-of-bounds Write vulnerability that could cause a Denial of Service on the Modicon PLC controller / simulator when updating the controller application with a specially crafted project file exists in Modicon M580 CPU (part numbers BMEP* and BMEH*, all versions), Modicon M340 CPU (part numbers BMXP34*, all versions), Modicon MC80 (part numbers BMKC80*, all versions), Modicon Momentum Ethernet CPU (part numbers 171CBU*, all versions), PLC Simulator for EcoStruxure ^a Control Expert, including all Unity Pro versions (former name of EcoStruxure ^a Control Expert, all versions), PLC Simulator for EcoStruxure ^a Process Expert including all HDCS versions (former name of EcoStruxure ^a Process Expert,	https://down load.schneide r- electric.com/f iles?p_Doc_Re f=SEVD- 2021-222-04	H-SCH-MODI- 180921/1997
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 & CVE ID	Patch	NCIIPC ID
			all versions), Modicon Quantum CPU (part numbers 140CPU*, all versions), Modicon Premium CPU (part numbers TSXP5*, all versions). CVE ID : CVE-2021-22791		
NULL Pointer Dereference	02-Sep-21	5	A CWE-476: NULL Pointer Dereference vulnerability that could cause a Denial of Service on the Modicon PLC controller / simulator when updating the controller application with a specially crafted project file exists in Modicon M580 CPU (part numbers BMEP* and BMEH*, all versions), Modicon M340 CPU (part numbers BMXP34*, all versions), Modicon MC80 (part numbers BMKC80*, all versions), Modicon Momentum Ethernet CPU (part numbers 171CBU*, all versions), PLC Simulator for EcoStruxure ^a Control Expert, including all Unity Pro versions (former name of EcoStruxure ^a Control Expert, all versions), PLC Simulator for EcoStruxure ^a Process Expert including all HDCS versions (former name of EcoStruxure ^a Process Expert, all versions), Modicon Quantum CPU (part numbers 140CPU*, all versions), Modicon Premium CPU (part numbers TSXP5*, all	https://down load.schneide r- electric.com/f iles?p_Doc_Re f=SEVD- 2021-222-04	H-SCH-MODI- 180921/1998
CVSS Scoring Sc	cale 0-1	1-2	2-3 3-4 4-5 5-6	6-7 7-8	8-9 9-10

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			versions).		
			CVE ID : CVE-2021-22792		
modicon_m5	80_bmep584	040			
Improper Restriction of Operations within the Bounds of a Memory Buffer	02-Sep-21	4	A CWE-119: Improper Restriction of Operations within the Bounds of a Memory Buffer vulnerability that could cause a Denial of Service on the Modicon PLC controller / simulator when updating the controller application with a specially crafted project file exists in Modicon M580 CPU (part numbers BMEP* and BMEH*, all versions), Modicon M340 CPU (part numbers BMXP34*, all versions), Modicon MC80 (part numbers BMKC80*, all versions), Modicon Momentum Ethernet CPU (part numbers 171CBU*, all versions), PLC Simulator for EcoStruxure ^a Control Expert, including all Unity Pro versions (former name of EcoStruxure ^a Control Expert, all versions), PLC Simulator for EcoStruxure ^a Process Expert including all HDCS versions (former name of EcoStruxure ^a Process Expert, all versions), Modicon Quantum CPU (part numbers 140CPU*, all versions), Modicon Premium CPU (part numbers TSXP5*, all versions).	https://down load.schneide r- electric.com/f iles?p_Doc_Re f=SEVD- 2021-222-04	H-SCH-MODI- 180921/1999

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2021-22789		
Out-of- bounds Read	02-Sep-21	4	A CWE-125: Out-of-bounds Read vulnerability that could cause a Denial of Service on the Modicon PLC controller / simulator when updating the controller application with a specially crafted project file exists in Modicon M580 CPU (part numbers BMEP* and BMEH*, all versions), Modicon M340 CPU (part numbers BMXP34*, all versions), Modicon MC80 (part numbers BMKC80*, all versions), Modicon Momentum Ethernet CPU (part numbers 171CBU*, all versions), PLC Simulator for EcoStruxure ^a Control Expert, including all Unity Pro versions (former name of EcoStruxure ^a Control Expert, all versions), PLC Simulator for EcoStruxure ^a Process Expert including all HDCS versions (former name of EcoStruxure ^a Process Expert, all versions), Modicon Quantum CPU (part numbers 140CPU*, all versions), Modicon Premium CPU (part numbers TSXP5*, all versions). CVE ID : CVE-2021-22790	https://down load.schneide r- electric.com/f iles?p_Doc_Re f=SEVD- 2021-222-04	H-SCH-MODI- 180921/2000
Out-of- bounds Write	02-Sep-21	4	A CWE-787: Out-of-bounds Write vulnerability that could cause a Denial of Service on the Modicon PLC controller /	https://down load.schneide r- electric.com/f	H-SCH-MODI- 180921/2001

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
			simulator when updating the controller application with a specially crafted project file exists in Modicon M580 CPU (part numbers BMEP* and BMEH*, all versions), Modicon M340 CPU (part numbers BMXP34*, all versions), Modicon MC80 (part numbers BMKC80*, all versions), Modicon Momentum Ethernet CPU (part numbers 171CBU*, all versions), PLC Simulator for EcoStruxure ^a Control Expert, including all Unity Pro versions (former name of EcoStruxure ^a Control Expert, all versions), PLC Simulator for EcoStruxure ^a Process Expert including all HDCS versions (former name of EcoStruxure ^a Process Expert, all versions), Modicon Quantum CPU (part numbers 140CPU*, all versions), Modicon Premium CPU (part numbers TSXP5*, all versions).	iles?p_Doc_Re f=SEVD- 2021-222-04	
NULL Pointer Dereference	02-Sep-21	5	CVE ID : CVE-2021-22791 A CWE-476: NULL Pointer Dereference vulnerability that could cause a Denial of Service on the Modicon PLC controller / simulator when updating the controller application with a specially crafted project file exists in Modicon M580 CPU (part numbers BMEP* and BMEH*,	https://down load.schneide r- electric.com/f iles?p_Doc_Re f=SEVD- 2021-222-04	H-SCH-MODI- 180921/2002

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			all versions), Modicon M340 CPU (part numbers BMXP34*, all versions), Modicon MC80 (part numbers BMKC80*, all versions), Modicon Momentum Ethernet CPU (part numbers 171CBU*, all versions), PLC Simulator for EcoStruxure ^a Control Expert, including all Unity Pro versions (former name of EcoStruxure ^a Control Expert, all versions), PLC Simulator for EcoStruxure ^a Process Expert including all HDCS versions (former name of EcoStruxure ^a Process Expert, all versions), Modicon Quantum CPU (part numbers 140CPU*, all versions), Modicon Premium CPU (part numbers TSXP5*, all versions). CVE ID : CVE-2021-22792		
modicon_m5	80 hmen584	040s			
Improper Restriction of Operations within the Bounds of a Memory Buffer	02-Sep-21	4	A CWE-119: Improper Restriction of Operations within the Bounds of a Memory Buffer vulnerability that could cause a Denial of Service on the Modicon PLC controller / simulator when updating the controller application with a specially crafted project file exists in Modicon M580 CPU (part numbers BMEP* and BMEH*, all versions), Modicon M340	https://down load.schneide r- electric.com/f iles?p_Doc_Re f=SEVD- 2021-222-04	H-SCH-MODI- 180921/2003

CVSS Scoring Scale	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10
Dago 747 of 1474										

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			CPU (part numbers BMXP34*, all versions), Modicon MC80 (part numbers BMKC80*, all versions), Modicon Momentum Ethernet CPU (part numbers 171CBU*, all versions), PLC Simulator for EcoStruxure ^a Control Expert, including all Unity Pro versions (former name of EcoStruxure ^a Control Expert, all versions), PLC Simulator for EcoStruxure ^a Process Expert including all HDCS versions (former name of EcoStruxure ^a Process Expert, all versions), Modicon EcoStruxure ^a Process Expert, all versions), Modicon (uantum CPU (part numbers 140CPU*, all versions), Modicon Premium CPU (part numbers TSXP5*, all versions).		
Out-of- bounds Read	02-Sep-21	4	A CWE-125: Out-of-bounds Read vulnerability that could cause a Denial of Service on the Modicon PLC controller / simulator when updating the controller application with a specially crafted project file exists in Modicon M580 CPU (part numbers BMEP* and BMEH*, all versions), Modicon M340 CPU (part numbers BMXP34*, all versions), Modicon MC80 (part numbers BMKC80*, all versions), Modicon	https://down load.schneide r- electric.com/f iles?p_Doc_Re f=SEVD- 2021-222-04	H-SCH-MODI- 180921/2004
CVSS Scoring Sc	ale 0-1	1-2	2-3 3-4 4-5 5-6	6-7 7-8	8-9 9-10

Out-of- bounds02-Sep-214(part numbers 171CBU*, all versions), PLC Simulator for EcoStruxure* Control Expert, all versions), PLC Simulator for EcoStruxure* Control Expert, all versions), PLC Simulator for EcoStruxure* Process Expert including all HDCS versions (former name of EcoStruxure* Process Expert, all versions), Modicon Quantum CPU (part numbers 140CPU*, all versions), Modicon Premium CPU (part numbers TSXP5*, all versions).+Out-of- boundsA CWE-787: Out-of-bounds write+Out-of- bounds WriteA CWE-787: Out-of-bounds wresions).+A CWE-787: Out-of-bounds wresions).+A CWE-787: Out-of-bounds wresions).+A CWE-787: Out-of-bounds wresions).+Bounds WriteA CWE-787: Out-of-bounds when updating the controller application with a specially crafted project file exists in Modicon MS80 CPU (part numbers BMKP8* and previsions). Modicon (part numbers BMK20*, all versions).+Out-of- bounds Write02-Sep-214Qut-of- bounds WriteModicon M340 CPU (part numbers BMK20*, all versions). Modicon Modicon MG00 versions). Modicon MG00 versions). Modicon MG00 versions). Modicon MG00 versions). Modicon MG00 versions). PLC Simulator for EcoStruxure* Control Expert, including all Unity Pro versions (former name of EcoStruxure* Control Expert, including all Unity Pro versions (former name of EcoStruxure* Control Expert, including all Unity Pro versions (former name of EcoStruxure* Control Expert, including all Unity Pro	Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Out-of- bounds02-Sep-214Write vulnerability that could cause a Denial of Service on the Modicon PLC controller / simulator when updating the controller application with a specially crafted project file exists in Modicon M580 CPU (part numbers BMEP* and BMEH*, all versions), Modicon M340 CPU (part numbers BMXP34*, all versions), Modicon MC800 (part numbers BMKC80*, all versions), Modicon MC800 (part numbers 171CBU*, all versions), PLC Simulator for EcoStruxureª Control Expert, including all Unity Pro versions (former name ofHttps://down load.schneide re electric.com/f iles?p_Doc_Re f=SEVD- 2021-222-04H-SCH-MODI- 180921/2005				versions), PLC Simulator for EcoStruxure ^a Control Expert, including all Unity Pro versions (former name of EcoStruxure ^a Control Expert, all versions), PLC Simulator for EcoStruxure ^a Process Expert including all HDCS versions (former name of EcoStruxure ^a Process Expert, all versions), Modicon Quantum CPU (part numbers 140CPU*, all versions), Modicon Premium CPU (part numbers TSXP5*, all versions).		
	bounds	02-Sep-21	4	Write vulnerability that could cause a Denial of Service on the Modicon PLC controller / simulator when updating the controller application with a specially crafted project file exists in Modicon M580 CPU (part numbers BMEP* and BMEH*, all versions), Modicon M340 CPU (part numbers BMXP34*, all versions), Modicon MC80 (part numbers BMKC80*, all versions), Modicon Momentum Ethernet CPU (part numbers 171CBU*, all versions), PLC Simulator for EcoStruxure ^a Control Expert, including all Unity Pro versions (former name of	load.schneide r- electric.com/f iles?p_Doc_Re f=SEVD-	

Page 749 of 1474

NULL Pointer Dereference02-Sep-215Adl versions including all versions), PLC Simulator for EcoStruxure ^a Process Expert including all HDCS versions (former name of EcoStruxure ^a Process Expert, all versions), Modicon Quantum CPU (part numbers 140CPU*, all versions), Modicon Premium CPU (part numbers TSXP5*, all versions). CVE ID : CVE-2021-22791Https://down loadscheid r electric.com/f iles*p_Doc_Re f=SEVD- 2021-222-04NULL Pointer Dereference02-Sep-215A CWE-476: NULL Pointer Dereference vulnerability that could cause a Denial of Service on the Modicon PLC controller / simulator when updating the controller application with a specially crafted project file exists in Modicon M580 CPU (part numbers BMEP* and BMEH*, all versions), Modicon M340 (Pu (part numbers BMXP34*, all versions), Modicon for EcoStruxure* Control Expert, including all Unity Pro versions (former name of EcoStruxure* Control Expert, all versions, PLC Simulator for EcoStruxure* Process Expert including all HDCS versions (former name of EcoStruxure* Process Expert, all versions, PLC Simulator for EcoStruxure* Process Expert including all HDCSH-SCH-MODI- lies*p_Doc_Re f=SEVD- 2021-222-04	Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
NULL Pointer DereferenceA CWE-476: NULL Pointer Dereference vulnerability that could cause a Denial of Service on the Modicon PLC controller / simulator when updating the controller application with a specially crafted project file exists in Modicon MS80 CPU (part numbers BMEP* and BMEH*, all versions), Modicon MS40 CPU (part numbers BMXP34*, all versions), Modicon MC80 (part numbers BMKC80*, all versions), Modicon Momentum Ethernet CPU (part numbers 171CBU*, all versions), PLC Simulator for EcoStruxure ^a Control Expert, including all Unity Pro versions (former name ofH-SCH-MODI- 180921/2006				for EcoStruxure ^a Process Expert including all HDCS versions (former name of EcoStruxure ^a Process Expert, all versions), Modicon Quantum CPU (part numbers 140CPU*, all versions), Modicon Premium CPU (part numbers TSXP5*, all versions).		
NULL Pointer DereferenceDereference vulnerability that could cause a Denial of Service on the Modicon PLC controller / simulator when updating the controller application with a specially crafted project file exists in Modicon M580 CPU (part numbers BMEP* and BMEH*, all versions), Modicon M340 CPU (part numbers BMXP34*, all versions), Modicon MC80 (part numbers BMKC80*, all versions), Modicon Momentum Ethernet CPU (part numbers 171CBU*, all versions), PLC Simulator for EcoStruxureª Control Expert, all versions), PLC Simulator for EcoStruxureª Control Expert, all versions), PLC Simulator for EcoStruxureª Process Expert including all HDCS versions (former name ofHttps://down load.schneide 						
	Pointer	02-Sep-21	5	Dereference vulnerability that could cause a Denial of Service on the Modicon PLC controller / simulator when updating the controller application with a specially crafted project file exists in Modicon M580 CPU (part numbers BMEP* and BMEH*, all versions), Modicon M340 CPU (part numbers BMXP34*, all versions), Modicon MC80 (part numbers BMKC80*, all versions), Modicon Momentum Ethernet CPU (part numbers 171CBU*, all versions), PLC Simulator for EcoStruxure ^a Control Expert, including all Unity Pro versions (former name of EcoStruxure ^a Process Expert including all HDCS versions (former name of	load.schneide r- electric.com/f iles?p_Doc_Re f=SEVD-	

Page 750 of 1474

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			all versions), Modicon Quantum CPU (part numbers 140CPU*, all versions), Modicon Premium CPU (part numbers TSXP5*, all versions). CVE ID : CVE-2021-22792		
modicon_m5	80_bmep585	040			
Improper Restriction of Operations within the Bounds of a Memory Buffer	02-Sep-21	4	A CWE-119: Improper Restriction of Operations within the Bounds of a Memory Buffer vulnerability that could cause a Denial of Service on the Modicon PLC controller / simulator when updating the controller application with a specially crafted project file exists in Modicon M580 CPU (part numbers BMEP* and BMEH*, all versions), Modicon M340 CPU (part numbers BMXP34*, all versions), Modicon MC80 (part numbers BMKC80*, all versions), Modicon Momentum Ethernet CPU (part numbers 171CBU*, all versions), PLC Simulator for EcoStruxure ^a Control Expert, including all Unity Pro versions (former name of EcoStruxure ^a Process Expert including all HDCS versions (former name of EcoStruxure ^a Process Expert, all versions), Modicon	https://down load.schneide r- electric.com/f iles?p_Doc_Re f=SEVD- 2021-222-04	H-SCH-MODI- 180921/2007

CVSS Scoring Scale	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10
Page 751 of 1474										

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Quantum CPU (part numbers 140CPU*, all versions), Modicon Premium CPU (part numbers TSXP5*, all versions). CVE ID : CVE-2021-22789		
Out-of- bounds Read	02-Sep-21	4	A CWE-125: Out-of-bounds Read vulnerability that could cause a Denial of Service on the Modicon PLC controller / simulator when updating the controller application with a specially crafted project file exists in Modicon M580 CPU (part numbers BMEP* and BMEH*, all versions), Modicon M340 CPU (part numbers BMXP34*, all versions), Modicon MC80 (part numbers BMKC80*, all versions), Modicon Momentum Ethernet CPU (part numbers 171CBU*, all versions), PLC Simulator for EcoStruxure ^a Control Expert, including all Unity Pro versions (former name of EcoStruxure ^a Control Expert, all versions), PLC Simulator for EcoStruxure ^a Process Expert including all HDCS versions (former name of EcoStruxure ^a Process Expert, all versions), Modicon Quantum CPU (part numbers 140CPU*, all versions), Modicon Premium CPU (part numbers TSXP5*, all versions).	https://down load.schneide r- electric.com/f iles?p_Doc_Re f=SEVD- 2021-222-04	H-SCH-MODI- 180921/2008

CVSS Scoring Scale	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10
			P	age 752 c	of 1474					

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2021-22790		
Out-of- bounds Write	02-Sep-21	4	A CWE-787: Out-of-bounds Write vulnerability that could cause a Denial of Service on the Modicon PLC controller / simulator when updating the controller application with a specially crafted project file exists in Modicon M580 CPU (part numbers BMEP* and BMEH*, all versions), Modicon M340 CPU (part numbers BMXP34*, all versions), Modicon MC80 (part numbers BMKC80*, all versions), Modicon MC80 (part numbers BMKC80*, all versions), Modicon Momentum Ethernet CPU (part numbers 171CBU*, all versions), PLC Simulator for EcoStruxure ^a Control Expert, including all Unity Pro versions (former name of EcoStruxure ^a Control Expert, all versions), PLC Simulator for EcoStruxure ^a Process Expert including all HDCS versions (former name of EcoStruxure ^a Process Expert, all versions), Modicon Quantum CPU (part numbers 140CPU*, all versions), Modicon Premium CPU (part numbers TSXP5*, all versions).	https://down load.schneide r- electric.com/f iles?p_Doc_Re f=SEVD- 2021-222-04	H-SCH-MODI- 180921/2009
NULL Pointer Dereference	02-Sep-21	5	A CWE-476: NULL Pointer Dereference vulnerability that could cause a Denial of Service on the Modicon PLC	https://down load.schneide r- electric.com/f	H-SCH-MODI- 180921/2010

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

Page 753 of 1474

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			controller / simulator when updating the controller application with a specially crafted project file exists in Modicon M580 CPU (part numbers BMEP* and BMEH*, all versions), Modicon M340 CPU (part numbers BMXP34*, all versions), Modicon MC80 (part numbers BMKC80*, all versions), Modicon Momentum Ethernet CPU (part numbers 171CBU*, all versions), PLC Simulator for EcoStruxure ^a Control Expert, including all Unity Pro versions (former name of EcoStruxure ^a Control Expert, all versions), PLC Simulator for EcoStruxure ^a Process Expert including all HDCS versions (former name of EcoStruxure ^a Process Expert, all versions), Modicon Quantum CPU (part numbers 140CPU*, all versions), Modicon Premium CPU (part numbers TSXP5*, all versions).	iles?p_Doc_Re f=SEVD- 2021-222-04	
modicon_m5	80_bmep585	040c			
Improper Restriction of Operations within the Bounds of a Memory	02-Sep-21	4	A CWE-119: Improper Restriction of Operations within the Bounds of a Memory Buffer vulnerability that could cause a Denial of Service on the Modicon PLC controller / simulator when	https://down load.schneide r- electric.com/f iles?p_Doc_Re f=SEVD- 2021-222-04	H-SCH-MODI- 180921/2011
CVSS Scoring Sco	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
Buffer			updating the controller application with a specially crafted project file exists in Modicon M580 CPU (part numbers BMEP* and BMEH*, all versions), Modicon M340 CPU (part numbers BMXP34*, all versions), Modicon MC80 (part numbers BMKC80*, all versions), Modicon Momentum Ethernet CPU (part numbers 171CBU*, all versions), PLC Simulator for EcoStruxure ^a Control Expert, including all Unity Pro versions (former name of EcoStruxure ^a Control Expert, all versions), PLC Simulator for EcoStruxure ^a Process Expert including all HDCS versions (former name of EcoStruxure ^a Process Expert, all versions), Modicon Quantum CPU (part numbers 140CPU*, all versions), Modicon Premium CPU (part numbers TSXP5*, all versions).		
Out-of- bounds Read	02-Sep-21	4	A CWE-125: Out-of-bounds Read vulnerability that could cause a Denial of Service on the Modicon PLC controller / simulator when updating the controller application with a specially crafted project file exists in Modicon M580 CPU (part numbers BMEP* and BMEH*, all versions),	https://down load.schneide r- electric.com/f iles?p_Doc_Re f=SEVD- 2021-222-04	H-SCH-MODI- 180921/2012 8-9 9-10

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Modicon M340 CPU (part numbers BMXP34*, all versions), Modicon MC80 (part numbers BMKC80*, all versions), Modicon Momentum Ethernet CPU (part numbers 171CBU*, all versions), PLC Simulator for EcoStruxure ^a Control Expert, including all Unity Pro versions (former name of EcoStruxure ^a Control Expert, all versions), PLC Simulator for EcoStruxure ^a Process Expert including all HDCS versions (former name of EcoStruxure ^a Process Expert, all versions), Modicon Quantum CPU (part numbers 140CPU*, all versions), Modicon Premium CPU (part numbers TSXP5*, all versions). CVE ID : CVE-2021-22790		
Out-of- bounds Write	02-Sep-21	4	A CWE-787: Out-of-bounds Write vulnerability that could cause a Denial of Service on the Modicon PLC controller / simulator when updating the controller application with a specially crafted project file exists in Modicon M580 CPU (part numbers BMEP* and BMEH*, all versions), Modicon M340 CPU (part numbers BMXP34*, all versions), Modicon MC80 (part numbers BMKC80*, all versions), Modicon	https://down load.schneide r- electric.com/f iles?p_Doc_Re f=SEVD- 2021-222-04	H-SCH-MODI- 180921/2013
CVSS Scoring Sc	ale 0-1	1-2	2-3 3-4 4-5 5-6	6-7 7-8	8-9 9-10

NULL Pointer Dereference02-Sep-215(part numbers 171CBU*, all versions), PLC Simulator for EcoStruxureª Control Expert, all versions), PLC Simulator for EcoStruxureª Process Expert including all HDCS versions (former name of EcoStruxureª Process Expert, all versions), Modicon Quantum CPU (part numbers 140CPU*, all versions), Modicon Premium CPU (part numbers TSXP5*, all versions).Https://down load schneide r electric.com/f iles?p.Doc.Re for Service on the Modicon PLC controller / simulator modicion WRP34*, all versions), Modicon MC80 (part numbers BMKC80*, all versions), Modicon MO400 (PU (part numbers all versions), Modicon M20 controller / simulator when updating the controller application with a specially crafted project file exists in Modicon M200 (PU topart numbers BMKC80*, all versions), Modicon M200 (PU (part numbers BMKC80*, all versions), Modicon MC80 (part numbers BMKC80*, all versions), Modicon Momentum Ethernet CPU (part numbers 171CBU*, all versions), PLC Simulator for EcoStruxureª Control Expert, including all Unity Pro versions (former name ofHttps://down load schneide r electric.com/f iles?p.Doc.Re fesEVD- 2021-222-04H-SCH-M0DI- iles?p.Doc.Re fesEVD- 2021-222-04	Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
NULL Pointer Dereference02-Sep-215Dereference vulnerability that could cause a Denial of Service on the Modicon PLC controller / simulator when updating the controller application with a specially crafted project file exists in numbers BMEP* and BMEH*, all versions), Modicon M340 CPU (part numbers BMXP34*, all versions), Modicon MC80 (part numbers BMKC80*, all versions), Modicon Modicon M000000000000000000000000000000000000				versions), PLC Simulator for EcoStruxure ^a Control Expert, including all Unity Pro versions (former name of EcoStruxure ^a Control Expert, all versions), PLC Simulator for EcoStruxure ^a Process Expert including all HDCS versions (former name of EcoStruxure ^a Process Expert, all versions), Modicon Quantum CPU (part numbers 140CPU*, all versions), Modicon Premium CPU (part numbers TSXP5*, all versions).		
CVSS Scoring Scale 0-1 1-2 2-3 3-4 4-5 5-6 6-7 7-8 8-9 9-10	Pointer Dereference			A CWE-476: NULL Pointer Dereference vulnerability that could cause a Denial of Service on the Modicon PLC controller / simulator when updating the controller application with a specially crafted project file exists in Modicon M580 CPU (part numbers BMEP* and BMEH*, all versions), Modicon M340 CPU (part numbers BMXP34*, all versions), Modicon MC80 (part numbers BMKC80*, all versions), Modicon Momentum Ethernet CPU (part numbers 171CBU*, all versions), PLC Simulator for EcoStruxure ^a Control Expert, including all Unity Pro versions (former name of	load.schneide r- electric.com/f iles?p_Doc_Re f=SEVD-	180921/2014

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			EcoStruxure ^ª Control Expert, all versions), PLC Simulator for EcoStruxure ^ª Process Expert including all HDCS versions (former name of EcoStruxure ^ª Process Expert, all versions), Modicon Quantum CPU (part numbers 140CPU*, all versions), Modicon Premium CPU (part numbers TSXP5*, all versions). CVE ID : CVE-2021-22792		
modicon_m5	80_bmep586	040			
Improper Restriction of Operations within the Bounds of a Memory Buffer	02-Sep-21	4	A CWE-119: Improper Restriction of Operations within the Bounds of a Memory Buffer vulnerability that could cause a Denial of Service on the Modicon PLC controller / simulator when updating the controller application with a specially crafted project file exists in Modicon M580 CPU (part numbers BMEP* and BMEH*, all versions), Modicon M340 CPU (part numbers BMXP34*, all versions), Modicon MC80 (part numbers BMKC80*, all versions), Modicon Momentum Ethernet CPU (part numbers 171CBU*, all versions), PLC Simulator for EcoStruxure ^a Control Expert, including all Unity Pro versions (former name of EcoStruxure ^a Control Expert,	https://down load.schneide r- electric.com/f iles?p_Doc_Re f=SEVD- 2021-222-04	H-SCH-MODI- 180921/2015

CVSS Scoring Scale	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10
			D	200 759 0	f 1/7/					

Out-of- bounds Read 02-Sep-21 4 A CWE-125: Out-of-bounds Read A CWE-125: Out-of-bounds Read https://down load.schneide r- scrisons), PLC Simulator for EcoStruxure* Process Expert, all versions), Modicon Quantum CPU (part numbers 140CPU*, all versions), Modicon Premium CPU (part numbers TSXP5*, all versions). A CWE-125: Out-of-bounds Read vulnerability that could cause a Denial of Service on the Modicon PLC controller / simulator when updating the controller application with a specially crafted project file exists in Modicon M580 CPU (part numbers BMK28*, all versions), Modicon M580 CPU (part numbers BMK28*, all versions), Modicon M580 (part numbers BMK28*, all versions), PLC Simulator for EcoStruxure* Control Expert, including all Unity Pro versions (former name of EcoStruxure* Process Expert including all HDCS versions (former name of EcoStruxure* Process Expert including all HDCS H-SCH-MODI- iles/p.Doc.Re for EcoStruxure* Process Expert including all HDCS	Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Out-of- bounds Read02-Sep-214A CWE-125: Out-of-bounds Read vulnerability that could cause a Denial of Service on the Modicon PLC controller / simulator when updating the controller application with a specially crafted project file exists in Modicon MS80 CPU (part numbers BMEP* and BMEH*, all versions), Modicon M340 CPU (part numbers BMXP34*, all versions), Modicon Modern M240 CPU (part numbers BMKC80*, all versions), Modicon (part numbers 171CBU*, all versions), PLC Simulator for EcoStruxure³ Control Expert, including all Unity Pro versions (former name of EcoStruxure³ Process Expert,https://down load.schneide r- electric.com/f iles?p_Doc_Re f=SEVD- 2021-222-04H-SCH-MODI- 180921/2016				for EcoStruxure ^ª Process Expert including all HDCS versions (former name of EcoStruxure ^ª Process Expert, all versions), Modicon Quantum CPU (part numbers 140CPU*, all versions), Modicon Premium CPU (part numbers TSXP5*, all		
Out-of- bounds02-Sep-214Read vulnerability that could cause a Denial of Service on the Modicon PLC controller / simulator when updating the controller application with a specially crafted project file exists in Modicon M580 CPU (part numbers BMEP* and BMEH*, all versions), Modicon M340 CPU (part numbers BMXP34*, all versions), Modicon MC80 (part numbers BMKC80*, all versions), Modicon Momentum Ethernet CPU (part numbers 171CBU*, all versions), PLC Simulator for EcoStruxureª Control Expert, all versions), PLC Simulator for EcoStruxureª Process Expert including all HDCS versions (former name of EcoStruxureª Process Expert,H-SCH-MODI- lase lase lase lase lase lase lase laseH-SCH-MODI- lase lase lase lase lase lase lase laseH-SCH-MODI- lase lase lase lase lase lase laseH-SCH-MODI- lase lase lase lase lase lase lase laseH-SCH-MODI- lase lase lase lase lase lase lase lase lase laseH-SCH-MODI- lase lase lase lase lase lase lase lase 				CVE ID : CVE-2021-22789		
	bounds	02-Sep-21	4	Read vulnerability that could cause a Denial of Service on the Modicon PLC controller / simulator when updating the controller application with a specially crafted project file exists in Modicon M580 CPU (part numbers BMEP* and BMEH*, all versions), Modicon M340 CPU (part numbers BMXP34*, all versions), Modicon MC80 (part numbers BMKC80*, all versions), Modicon Momentum Ethernet CPU (part numbers 171CBU*, all versions), PLC Simulator for EcoStruxure ^a Control Expert, including all Unity Pro versions (former name of EcoStruxure ^a Process Expert including all HDCS versions (former name of	load.schneide r- electric.com/f iles?p_Doc_Re f=SEVD-	

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Quantum CPU (part numbers 140CPU*, all versions), Modicon Premium CPU (part numbers TSXP5*, all versions). CVE ID : CVE-2021-22790		
Out-of- bounds Write	02-Sep-21	4	A CWE-787: Out-of-bounds Write vulnerability that could cause a Denial of Service on the Modicon PLC controller / simulator when updating the controller application with a specially crafted project file exists in Modicon M580 CPU (part numbers BMEP* and BMEH*, all versions), Modicon M340 CPU (part numbers BMXP34*, all versions), Modicon MC80 (part numbers BMKC80*, all versions), Modicon Momentum Ethernet CPU (part numbers 171CBU*, all versions), PLC Simulator for EcoStruxure ^a Control Expert, including all Unity Pro versions (former name of EcoStruxure ^a Control Expert, all versions), PLC Simulator for EcoStruxure ^a Process Expert including all HDCS versions (former name of EcoStruxure ^a Process Expert, all versions), Modicon Quantum CPU (part numbers 140CPU*, all versions), Modicon Premium CPU (part numbers TSXP5*, all versions).	https://down load.schneide r- electric.com/f iles?p_Doc_Re f=SEVD- 2021-222-04	H-SCH-MODI- 180921/2017

CVSS Scoring Scale	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10
			P	age 760 c	of 1474					

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
of Operations within the Bounds of a Memory Buffer			<pre>within the Bounds of a Memory Buffer vulnerability that could cause a Denial of Service on the Modicon PLC controller / simulator when updating the controller application with a specially crafted project file exists in Modicon M580 CPU (part numbers BMEP* and BMEH*, all versions), Modicon M340 CPU (part numbers BMXP34*, all versions), Modicon MC80 (part numbers BMKC80*, all versions), Modicon Momentum Ethernet CPU (part numbers 171CBU*, all versions), PLC Simulator for EcoStruxure^a Control Expert, including all Unity Pro versions (former name of EcoStruxure^a Control Expert, all versions), PLC Simulator for EcoStruxure^a Process Expert including all HDCS versions (former name of EcoStruxure^a Process Expert, all versions), Modicon Quantum CPU (part numbers 140CPU*, all versions), Modicon Premium CPU (part numbers TSXP5*, all versions). CVE ID : CVE-2021-22789</pre>	r- electric.com/f iles?p_Doc_Re f=SEVD- 2021-222-04	
Out-of- bounds Read CVSS Scoring Sc	02-Sep-21	4	A CWE-125: Out-of-bounds Read vulnerability that could cause a Denial of Service on the Modicon PLC controller / simulator when updating the 2-3 3-4 4-5 5-6	https://down load.schneide r- electric.com/f iles?p_Doc_Re 6-7 7-8	H-SCH-MODI- 180921/2020 8-9 9-10

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			controller application with a specially crafted project file exists in Modicon M580 CPU (part numbers BMEP* and BMEH*, all versions), Modicon M340 CPU (part numbers BMXP34*, all versions), Modicon MC80 (part numbers BMKC80*, all versions), Modicon Momentum Ethernet CPU (part numbers 171CBU*, all versions), PLC Simulator for EcoStruxure ^a Control Expert, including all Unity Pro versions (former name of EcoStruxure ^a Control Expert, all versions), PLC Simulator for EcoStruxure ^a Process Expert including all HDCS versions (former name of EcoStruxure ^a Process Expert, all versions), Modicon Quantum CPU (part numbers 140CPU*, all versions), Modicon Premium CPU (part numbers TSXP5*, all versions).	f=SEVD- 2021-222-04	
Out-of- bounds Write	02-Sep-21	4	A CWE-787: Out-of-bounds Write vulnerability that could cause a Denial of Service on the Modicon PLC controller / simulator when updating the controller application with a specially crafted project file exists in Modicon M580 CPU (part numbers BMEP* and BMEH*, all versions), Modicon M340 CPU (part	https://down load.schneide r- electric.com/f iles?p_Doc_Re f=SEVD- 2021-222-04	H-SCH-MODI- 180921/2021

NULL 02-Sep-21 5 A CWE-476: NULL Pointer Dereference A CWE-476: NULL Pointer Dereference https://down load.schneide r- controller / simulator when updating the controller / simulator for EcoStruxure* Control Expert, including all Unity Proversions, PLC Simulator for EcoStruxure* Control Expert, all versions), PLC Simulator for EcoStruxure* Control Expert, all versions), Nodicon NULL 02-Sep-21 5 A CWE-476: NULL Pointer Dereference H-SCH-MODI-Topic Project file exists in Modicon M340 (part numbers BMEP* and BMEP*, all versions), Modicon https://down load.schneide r- controller / simulator when updating the controller all versions), Modicon M340 (part numbers BMEP*, all versions), Modicon M340 (part numbers BMK284*, all versions), Modicon M280 (part numbers MK284*, all versions), Modicon M280 (part numb	Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
NULL Pointer DereferenceDereference vulnerability that could cause a Denial of Service on the Modicon PLC controller / simulator when updating the controller application with a speciallyhttps://down load.schneide electric.com/f iles?p_Doc_Re f=SEVD- 2021-222-04H-SCH-MODI- 180921/2022NULL Pointer Dereference02-Sep-215Modicon M580 CPU (part numbers BMEP* and BMEH*, all versions), Modicon M340 CPU (part numbers BMXP34*, all versions), Modicon MC80 (part numbers BMKC80*, all versions), Modiconr- electric.com/f iles?p_Doc_Re f=SEVD- 2021-222-04H-SCH-MODI- 180921/2022				versions), Modicon MC80 (part numbers BMKC80*, all versions), Modicon Momentum Ethernet CPU (part numbers 171CBU*, all versions), PLC Simulator for EcoStruxure ^a Control Expert, including all Unity Pro versions (former name of EcoStruxure ^a Control Expert, all versions), PLC Simulator for EcoStruxure ^a Process Expert including all HDCS versions (former name of EcoStruxure ^a Process Expert, all versions), Modicon Quantum CPU (part numbers 140CPU*, all versions), Modicon Premium CPU (part numbers TSXP5*, all versions).		
Momentum Ethernet CPU	Pointer	02-Sep-21	5	Dereference vulnerability that could cause a Denial of Service on the Modicon PLC controller / simulator when updating the controller application with a specially crafted project file exists in Modicon M580 CPU (part numbers BMEP* and BMEH*, all versions), Modicon M340 CPU (part numbers BMXP34*, all versions), Modicon MC80 (part numbers BMKC80*, all versions), Modicon	load.schneide r- electric.com/f iles?p_Doc_Re f=SEVD-	

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			(part numbers 171CBU*, all versions), PLC Simulator for EcoStruxure ^a Control Expert, including all Unity Pro versions (former name of EcoStruxure ^a Control Expert, all versions), PLC Simulator for EcoStruxure ^a Process Expert including all HDCS versions (former name of EcoStruxure ^a Process Expert, all versions), Modicon Quantum CPU (part numbers 140CPU*, all versions), Modicon Premium CPU (part numbers TSXP5*, all versions). CVE ID : CVE-2021-22792		
modicon_mc	80_bmkc802	0301			
Improper Restriction of Operations within the Bounds of a Memory Buffer	02-Sep-21	4	A CWE-119: Improper Restriction of Operations within the Bounds of a Memory Buffer vulnerability that could cause a Denial of Service on the Modicon PLC controller / simulator when updating the controller application with a specially crafted project file exists in Modicon M580 CPU (part numbers BMEP* and BMEH*, all versions), Modicon M340 CPU (part numbers BMXP34*, all versions), Modicon MC80 (part numbers BMKC80*, all versions), Modicon Momentum Ethernet CPU (part numbers 171CBU*, all	https://down load.schneide r- electric.com/f iles?p_Doc_Re f=SEVD- 2021-222-04	H-SCH-MODI- 180921/2023

CVSS Scoring Scale	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-1
			P	age 765 c	of 1474					

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			versions), PLC Simulator for EcoStruxure ^a Control Expert, including all Unity Pro versions (former name of EcoStruxure ^a Control Expert, all versions), PLC Simulator for EcoStruxure ^a Process Expert including all HDCS versions (former name of EcoStruxure ^a Process Expert, all versions), Modicon Quantum CPU (part numbers 140CPU*, all versions), Modicon Premium CPU (part numbers TSXP5*, all versions). CVE ID : CVE-2021-22789		
Out-of- bounds Read	02-Sep-21	4	A CWE-125: Out-of-bounds Read vulnerability that could cause a Denial of Service on the Modicon PLC controller / simulator when updating the controller application with a specially crafted project file exists in Modicon M580 CPU (part numbers BMEP* and BMEH*, all versions), Modicon M340 CPU (part numbers BMXP34*, all versions), Modicon MC80 (part numbers BMKC80*, all versions), Modicon Momentum Ethernet CPU (part numbers 171CBU*, all versions), PLC Simulator for EcoStruxure ^a Control Expert, including all Unity Pro versions (former name of EcoStruxure ^a Control Expert, all versions), PLC Simulator	https://down load.schneide r- electric.com/f iles?p_Doc_Re f=SEVD- 2021-222-04	H-SCH-MODI- 180921/2024

Out-of- bounds02-Sep-214for EcoStruxureª Process Expert including all HDCS versions (former name of EcoStruxureª Process Expert, all versions), Modicon Quantum CPU (part numbers 140CPU*, all versions), Modicon Premium CPU (part numbers TSXP5*, all versions).VertionCVE D: CVE-2021-22790VertionCVE D: CVE-2021-22790VertionA CWE-787: Out-of-bounds Write vulnerability that could cause a Denial of Service on the Modicon PLC controller / simulator when updating the controller application with a specially crafted project file exists in Modicon MS80 CPU (part numbers BMEP* and BMEH*, all versions), Modicon MG80 CPU (part numbers BMKP34*, all versions), Modicon Modicon M340 CPU (part numbers T17LBU*, all versions), Modicon iles?p.Doc_Re (FSEVD- 2021-222-04H-SCH-MODI- 180921/2025Write02-Sep-214Kersions), PLC Simulator for EcoStruxure* Control Expert, all versions), PLC Simulator for EcoStruxure* Process Expert including all HDCS versions (former name of EcoStruxure* Process Expert including all HDCSH-SCH-MODI- ils*P_Doc_Re (SUP)	Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Out-of- bounds02-Sep-214Write vulnerability that could cause a Denial of Service on the Modicon PLC controller / simulator when updating the controller application with a specially crafted project file exists in Modicon M580 CPU (part numbers BMEP* and BMEH*, all versions), Modicon M340 CPU (part numbers BMXP34*, all versions), Modicon M680 (part numbers BMKC80*, all r- iles?p_Doc_Re (part numbers 171CBU*, all versions), PLC Simulator for EcoStruxure ^a Control Expert, all versions), PLC Simulator for EcoStruxure ^a Process Expert including all HDCS versions), ModiconH-SCH-MODI- 180921/2025				Expert including all HDCS versions (former name of EcoStruxure ^a Process Expert, all versions), Modicon Quantum CPU (part numbers 140CPU*, all versions), Modicon Premium CPU (part numbers TSXP5*, all versions).		
CVSS Scoring Scale 0-1 1-2 2-3 3-4 4-5 5-6 6-7 7-8 8-9 9-10	bounds	02-Sep-21	4	Write vulnerability that could cause a Denial of Service on the Modicon PLC controller / simulator when updating the controller application with a specially crafted project file exists in Modicon M580 CPU (part numbers BMEP* and BMEH*, all versions), Modicon M340 CPU (part numbers BMXP34*, all versions), Modicon MC80 (part numbers BMKC80*, all versions), Modicon MC80 (part numbers BMKC80*, all versions), Modicon Momentum Ethernet CPU (part numbers 171CBU*, all versions), PLC Simulator for EcoStruxure ^a Control Expert, including all Unity Pro versions (former name of EcoStruxure ^a Control Expert, all versions), PLC Simulator for EcoStruxure ^a Process Expert including all HDCS versions (former name of EcoStruxure ^a Process Expert, all versions), Modicon Quantum CPU (part numbers	load.schneide r- electric.com/f iles?p_Doc_Re f=SEVD-	

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Weakness	Publish Date	CVSS	140CPU*, all versions), Modicon Premium CPU (part numbers TSXP5*, all versions). CVE ID : CVE-2021-22791 A CWE-476: NULL Pointer Dereference vulnerability that could cause a Denial of Service on the Modicon PLC controller / simulator when updating the controller application with a specially crafted project file exists in Modicon M580 CPU (part numbers BMEP* and BMEH*, all versions), Modicon M340 CPU (part numbers BMXP34*, all versions),	Patch	NCIIPC ID
NULL Pointer Dereference	02-Sep-21	5		https://down load.schneide r- electric.com/f iles?p_Doc_Re f=SEVD- 2021-222-04	H-SCH-MODI- 180921/2026

CVSS Scoring Scale	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10
			Р	age 768 c	of 1474					

Improper Restriction of Operations within the Bestriction of Operations 02-Sep-21 A A CWE-119: Improper Restriction of Operations within the Bounds of a Memory Buffer vulnerability that could cause a Denial of Service on the Modicon PLC controller / simulator when updating the controller application with a specially crafted project file exists in Modicon MS80 CPU (part numbers BMEP* and BMEH*, all versions), Modicon M340 CPU (part numbers BMXP34*, all versions), Modicon MC80 (part numbers BMKC80*, all versions), Modicon Momentum Ethernet CPU (part numbers 171CBU*, all versions), PLC Simulator for EcoStruxure ⁸ Control Expert, all versions), PLC Simulator for EcoStruxure ⁸ Process Expert including all Unity Pro versions (former name of EcoStruxure ⁸ Process Expert including all HDCS versions), Modicon Quantum CPU (part numbers 140CPU*, all versions), Modicon PLC Versions), Modicon H-SCH-MODI- 180921/2027 F5EVD- 2021-222-04 H-SCH-MODI- 180921/2027
Improper Restriction of Operations within the Bounds of a Memory Buffer vulnerability that could cause a Denial of Service on the Modicon PLC controller / simulator when updating the controller application with a specially crafted project file exists in Modicon M580 CPU (part numbers BMEP* and BMEH*, all versions), Modicon M340 CPU (part numbers BMXP34*, all versions), Modicon MC80 (part numbers BMKC80*, all versions), Modicon EcoStruxure* Control Expert, including all Unity Pro versions (former name of EcoStruxure* Control Expert, all versions), PLC Simulator for EcoStruxure* Process Expert including all HDCS versions, Modicon Quantum CPU (part numbers 140CPU*, all versions), Modicon Quantum CPU (part numbers 140CPU*, all versions), ModiconH+SCH-MODI- 180921/2027 180921/2027 180921/2027
Improper Restriction of Operations within the Bounds of a Memory Buffer vulnerability that could cause a Denial of Service on the Modicon PLC controller / simulator when updating the controller application with a specially crafted project file exists in Modicon M580 CPU (part numbers BMEP* and BMEH*, all versions), Modicon M340 CPU (part numbers BMXP34*, all versions), Modicon M260 (part numbers BMK260*, all versions), Modiconhttps://down load.schneide r- electric.com/f ies?p.Doc.Re f=SEVD- 2021-222-04H-SCH-MODI- 180921/2027Improper Restriction of Operations within the
CVE ID : CVE-2021-22789

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Out-of- bounds Read	02-Sep-21	4	A CWE-125: Out-of-bounds Read vulnerability that could cause a Denial of Service on the Modicon PLC controller / simulator when updating the controller application with a specially crafted project file exists in Modicon M580 CPU (part numbers BMEP* and BMEH*, all versions), Modicon M340 CPU (part numbers BMXP34*, all versions), Modicon MC80 (part numbers BMKC80*, all versions), Modicon MC80 (part numbers BMKC80*, all versions), Modicon Momentum Ethernet CPU (part numbers 171CBU*, all versions), PLC Simulator for EcoStruxure ^a Control Expert, including all Unity Pro versions (former name of EcoStruxure ^a Control Expert, all versions), PLC Simulator for EcoStruxure ^a Process Expert including all HDCS versions (former name of EcoStruxure ^a Process Expert, all versions), Modicon Quantum CPU (part numbers 140CPU*, all versions), Modicon Premium CPU (part numbers TSXP5*, all versions).	https://down load.schneide r- electric.com/f iles?p_Doc_Re f=SEVD- 2021-222-04	H-SCH-MODI- 180921/2028
Out-of- bounds Write	02-Sep-21	4	A CWE-787: Out-of-bounds Write vulnerability that could cause a Denial of Service on the Modicon PLC controller / simulator when updating the controller application with a	https://down load.schneide r- electric.com/f iles?p_Doc_Re f=SEVD-	H-SCH-MODI- 180921/2029

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			specially crafted project file exists in Modicon M580 CPU (part numbers BMEP* and BMEH*, all versions), Modicon M340 CPU (part numbers BMXP34*, all versions), Modicon MC80 (part numbers BMKC80*, all versions), Modicon Momentum Ethernet CPU (part numbers 171CBU*, all versions), PLC Simulator for EcoStruxure ^a Control Expert, including all Unity Pro versions (former name of EcoStruxure ^a Control Expert, all versions), PLC Simulator for EcoStruxure ^a Process Expert including all HDCS versions (former name of EcoStruxure ^a Process Expert, all versions), Modicon Versions (former name of EcoStruxure ^a Process Expert, all versions), Modicon Quantum CPU (part numbers 140CPU*, all versions), Modicon Premium CPU (part numbers TSXP5*, all versions).	2021-222-04	
NULL Pointer Dereference	02-Sep-21	5	A CWE-476: NULL Pointer Dereference vulnerability that could cause a Denial of Service on the Modicon PLC controller / simulator when updating the controller application with a specially crafted project file exists in Modicon M580 CPU (part numbers BMEP* and BMEH*, all versions), Modicon M340 CPU (part numbers	https://down load.schneide r- electric.com/f iles?p_Doc_Re f=SEVD- 2021-222-04	H-SCH-MODI- 180921/2030

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			BMXP34*, all versions), Modicon MC80 (part numbers BMKC80*, all versions), Modicon Momentum Ethernet CPU (part numbers 171CBU*, all versions), PLC Simulator for EcoStruxure ^a Control Expert, including all Unity Pro versions (former name of EcoStruxure ^a Control Expert, all versions), PLC Simulator for EcoStruxure ^a Process Expert including all HDCS versions (former name of EcoStruxure ^a Process Expert, all versions), Modicon Quantum CPU (part numbers 140CPU*, all versions), Modicon Premium CPU (part numbers TSXP5*, all versions). CVE ID : CVE-2021-22792		
modicon_mc	80_bmkc803	0311		1	
Improper Restriction of Operations within the Bounds of a Memory Buffer	02-Sep-21	4	A CWE-119: Improper Restriction of Operations within the Bounds of a Memory Buffer vulnerability that could cause a Denial of Service on the Modicon PLC controller / simulator when updating the controller application with a specially crafted project file exists in Modicon M580 CPU (part numbers BMEP* and BMEH*, all versions), Modicon M340 CPU (part numbers BMXP34*, all versions),	https://down load.schneide r- electric.com/f iles?p_Doc_Re f=SEVD- 2021-222-04	H-SCH-MODI- 180921/2031

CVSS Scoring Scale	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10
			P	age 772 c	of 1474					

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Modicon MC80 (part numbers BMKC80*, all versions), Modicon Momentum Ethernet CPU (part numbers 171CBU*, all versions), PLC Simulator for EcoStruxure ^a Control Expert, including all Unity Pro versions (former name of EcoStruxure ^a Control Expert, all versions), PLC Simulator for EcoStruxure ^a Process Expert including all HDCS versions (former name of EcoStruxure ^a Process Expert, all versions), Modicon Quantum CPU (part numbers 140CPU*, all versions), Modicon Premium CPU (part numbers TSXP5*, all versions).		
Out-of- bounds Read	02-Sep-21	4	A CWE-125: Out-of-bounds Read vulnerability that could cause a Denial of Service on the Modicon PLC controller / simulator when updating the controller application with a specially crafted project file exists in Modicon M580 CPU (part numbers BMEP* and BMEH*, all versions), Modicon M340 CPU (part numbers BMXP34*, all versions), Modicon MC80 (part numbers BMKC80*, all versions), Modicon Momentum Ethernet CPU (part numbers 171CBU*, all versions), PLC Simulator for	https://down load.schneide r- electric.com/f iles?p_Doc_Re f=SEVD- 2021-222-04	H-SCH-MODI- 180921/2032

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			EcoStruxure ^ª Control Expert, including all Unity Pro versions (former name of EcoStruxure ^ª Control Expert, all versions), PLC Simulator for EcoStruxure ^ª Process Expert including all HDCS versions (former name of EcoStruxure ^ª Process Expert, all versions), Modicon Quantum CPU (part numbers 140CPU*, all versions), Modicon Premium CPU (part numbers TSXP5*, all versions). CVE ID : CVE-2021-22790		
Out-of- bounds Write	02-Sep-21	4	A CWE-787: Out-of-bounds Write vulnerability that could cause a Denial of Service on the Modicon PLC controller / simulator when updating the controller application with a specially crafted project file exists in Modicon M580 CPU (part numbers BMEP* and BMEH*, all versions), Modicon M340 CPU (part numbers BMXP34*, all versions), Modicon MC80 (part numbers BMKC80*, all versions), Modicon Momentum Ethernet CPU (part numbers 171CBU*, all versions), PLC Simulator for EcoStruxure ^a Control Expert, including all Unity Pro versions (former name of EcoStruxure ^a Control Expert, all versions), PLC Simulator for EcoStruxure ^a Process	https://down load.schneide r- electric.com/f iles?p_Doc_Re f=SEVD- 2021-222-04	H-SCH-MODI- 180921/2033

NULL Pointer Dereference02-Sep-215Expert including all HDCS versions (former name of EcoStruxure ⁴ Process Expert, all versions), Modicon Quantum CPU (part numbers 140CPU*, all versions), Modicon Premium CPU (part numbers TSXP5*, all versions). CVE ID : CVE-2021-22791Here Processes Processe Pr	Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
NULL Pointer Dereference02-Sep-215Dereference vulnerability that could cause a Denial of Service on the Modicon PLC controller / simulator when updating the controller application with a specially crafted project file exists in Modicon M580 CPU (part numbers BMEP* and BMEH*, all versions), Modicon M340 CPU (part numbers BMXP34*, all versions), Modicon MC80 (part numbers BMKC80*, all versions), Modiconhttps://down load.schneide r- electric.com/f iles?p_Doc_Re f=SEVD- 2021-222-04H-SCH-MODI- 180921/2034NULL Pointer Dereference02-Sep-215Modicon MC80 (part numbers BMKC80*, all versions), Modiconhttps://down load.schneide r- electric.com/f iles?p_Doc_Re f=SEVD- 2021-222-04H-SCH-MODI- 180921/2034IB0921/2034 including all Unity Pro versions (former name of EcoStruxureª Control Expert, all versions), PLC Simulator for EcoStruxureª Process Expert including all HDCS versions (former name of EcoStruxureª Process Expert, all versions), ModiconH-SCH-MODI- iles?p_Doc_Re f=SEVD- 2021-222-04				versions (former name of EcoStruxure ^a Process Expert, all versions), Modicon Quantum CPU (part numbers 140CPU*, all versions), Modicon Premium CPU (part numbers TSXP5*, all versions).		
	Pointer	02-Sep-21	5	Dereference vulnerability that could cause a Denial of Service on the Modicon PLC controller / simulator when updating the controller application with a specially crafted project file exists in Modicon M580 CPU (part numbers BMEP* and BMEH*, all versions), Modicon M340 CPU (part numbers BMXP34*, all versions), Modicon MC80 (part numbers BMKC80*, all versions), Modicon Momentum Ethernet CPU (part numbers 171CBU*, all versions), PLC Simulator for EcoStruxure ^a Control Expert, including all Unity Pro versions (former name of EcoStruxure ^a Control Expert, all versions), PLC Simulator for EcoStruxure ^a Process Expert including all HDCS versions (former name of EcoStruxure ^a Process Expert, all versions), Modicon	load.schneide r- electric.com/f iles?p_Doc_Re f=SEVD-	

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
modicon_mo	mentum_171	cbu78			
Improper Restriction of Operations within the Bounds of a Memory Buffer	02-Sep-21	4	A CWE-119: Improper Restriction of Operations within the Bounds of a Memory Buffer vulnerability that could cause a Denial of Service on the Modicon PLC controller / simulator when updating the controller application with a specially crafted project file exists in Modicon M580 CPU (part numbers BMEP* and BMEH*, all versions), Modicon M340 CPU (part numbers BMXP34*, all versions), Modicon MC80 (part numbers BMKC80*, all versions), Modicon Momentum Ethernet CPU (part numbers 171CBU*, all versions), PLC Simulator for EcoStruxure ^a Control Expert, including all Unity Pro versions (former name of EcoStruxure ^a Control Expert, all versions), PLC Simulator for EcoStruxure ^a Process Expert including all HDCS versions (former name of EcoStruxure ^a Process Expert, all versions), Modicon Quantum CPU (part numbers 140CPU*, all versions),	https://down load.schneide r- electric.com/f iles?p_Doc_Re f=SEVD- 2021-222-04	H-SCH-MODI- 180921/2035

CVSS Scoring Scale	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10
5			D	200 776 0	£1171					

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Weakness Out-of- bounds Read	Publish Date	CVSS	Description & CVE IDModicon Premium CPU (partnumbers TSXP5*, allversions).CVE ID : CVE-2021-22789A CWE-125: Out-of-boundsRead vulnerability that couldcause a Denial of Service onthe Modicon PLC controller /simulator when updating thecontroller application with aspecially crafted project fileexists in Modicon M580 CPU(part numbers BMEP* andBMEH*, all versions),Modicon M340 CPU (partnumbers BMXP34*, allversions), Modicon MC80(part numbers BMKC80*, allversions), ModiconMomentum Ethernet CPU(part numbers 171CBU*, allversions), PLC Simulator forEcoStruxure ^a Control Expert,including all Unity Proversions), PLC Simulatorfor EcoStruxure ^a ProcessExpert including all HDCSversions (former name ofEcoStruxure ^a Process Expert,all versions), ModiconQuantum CPU (part numbers140CPU*, all versions),Modicon Premium CPU (partnumbers TSXP5*, all	Patch https://down load.schneide r- electric.com/f iles?p_Doc_Re f=SEVD- 2021-222-04	NCIIPC ID
			versions). CVE ID : CVE-2021-22790		
Out-of-	02-Sep-21	4	A CWE-787: Out-of-bounds	https://down	H-SCH-MODI-

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
bounds Write			Write vulnerability that could cause a Denial of Service on the Modicon PLC controller / simulator when updating the controller application with a specially crafted project file exists in Modicon M580 CPU (part numbers BMEP* and BMEH*, all versions), Modicon M340 CPU (part numbers BMXP34*, all versions), Modicon MC80 (part numbers BMKC80*, all versions), Modicon MC80 (part numbers BMKC80*, all versions), Modicon Momentum Ethernet CPU (part numbers 171CBU*, all versions), PLC Simulator for EcoStruxure ^a Control Expert, including all Unity Pro versions (former name of EcoStruxure ^a Control Expert, all versions), PLC Simulator for EcoStruxure ^a Process Expert including all HDCS versions (former name of EcoStruxure ^a Process Expert, all versions), Modicon Quantum CPU (part numbers 140CPU*, all versions), Modicon Premium CPU (part numbers TSXP5*, all versions).	load.schneide r- electric.com/f iles?p_Doc_Re f=SEVD- 2021-222-04	180921/2037
NULL Pointer Dereference CVSS Scoring Sc	02-Sep-21 ale 0-1	5	A CWE-476: NULL Pointer Dereference vulnerability that could cause a Denial of Service on the Modicon PLC controller / simulator when updating the controller application with a specially 2-3 3-4 4-5 5-6	https://down load.schneide r- electric.com/f iles?p_Doc_Re f=SEVD-	H-SCH-MODI- 180921/2038 8-9 9-10

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			crafted project file exists in Modicon M580 CPU (part numbers BMEP* and BMEH*, all versions), Modicon M340 CPU (part numbers BMXP34*, all versions), Modicon MC80 (part numbers BMKC80*, all versions), Modicon Momentum Ethernet CPU (part numbers 171CBU*, all versions), PLC Simulator for EcoStruxure ^a Control Expert, including all Unity Pro versions (former name of EcoStruxure ^a Control Expert, all versions), PLC Simulator for EcoStruxure ^a Process Expert including all HDCS versions (former name of EcoStruxure ^a Process Expert, all versions), Modicon Quantum CPU (part numbers 140CPU*, all versions), Modicon Premium CPU (part numbers TSXP5*, all versions). CVE ID : CVE-2021-22792	2021-222-04	
modicon_mo	mentum_171	cbu98	090		
Improper Restriction of Operations within the Bounds of a Memory Buffer	02-Sep-21	4	A CWE-119: Improper Restriction of Operations within the Bounds of a Memory Buffer vulnerability that could cause a Denial of Service on the Modicon PLC controller / simulator when updating the controller application with a specially crafted project file exists in	https://down load.schneide r- electric.com/f iles?p_Doc_Re f=SEVD- 2021-222-04	H-SCH-MODI- 180921/2039

_											
	CVSS Scoring Scale	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10
_	Page 779 of 1474										

Out-of- bounds02-Sep-214Modicon M580 CPU (part numbers BMEP* and BMEH*, all versions), Modicon M340 CPU (part numbers BMXP34*, all versions), Modicon MC80 (part numbers BMKC80*, all versions), Modicon Momentum Ethernet CPU (part numbers 171CBU*, all versions), PLC Simulator for EcoStruxure* Control Expert, including all Unity Pro versions), PLC Simulator for EcoStruxure* Control Expert, all versions), PLC Simulator for EcoStruxure* Process Expert including all HDCS versions), Modicon Quantum CPU (part numbers 140CPU*, all versions), Modicon Quantum CPU (part numbers STXP5*, all versions).https://down load.schneid r- electric.com/f iles?p.Doc.Re f=SFUD_ 2021-222-04https://down load.schneid r- electric.com/f iles?p.Doc.Re f=SFUD_ 2021-222-04https://down load.schneid r- electric.com/f iles?p.Doc.Re f=SFUD_ 2021-222-04https://down load.schneid r- electric.com/f iles?p.Doc.Re f=SFUD_ 2021-222-04https://down load.schneid r- electric.com/f iles?p.Doc.Re f=SFUD_ 2021-222-04https://down load.schneid r- electric.com/f iles?p.Doc.Re f=SFUD_ 2021-222-04https://down load.schneid r- electric.com/f iles?p.Doc.Re f=SFUD_ 2021-222-04https://down load.schneid r- electric.com/f iles?p.Doc.Re f=SFUD_ 2021-222-04https://down load.schneid r- electric.com/f iles?p.Doc.Re f=SFUD_ 2021-222-04https://down load.schneid r- electric.com/f iles?p.Doc.Re f=SFUD_ 2021-222-04https://down load.schneid r- electric.com/f iles?p.Doc.Re f=SFUD_ 2021-222-04https://down load.schneid r- electric.com/f iles?p.Doc.Re f=SFUD_ 202	Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Out-of- bounds Read02-Sep-214Read vulnerability that could cause a Denial of Service on the Modicon PLC controller / simulator when updating the controller application with a specially crafted project file exists in Modicon M580 CPU (part numbers BMEP* and BMEH*, all versions),https://down load.schneide electric.com/f iles?p_Doc_Re f=SEVD- 2021-222-04H-SCH-MODI- 180921/2040				numbers BMEP* and BMEH*, all versions), Modicon M340 CPU (part numbers BMXP34*, all versions), Modicon MC80 (part numbers BMKC80*, all versions), Modicon Momentum Ethernet CPU (part numbers 171CBU*, all versions), PLC Simulator for EcoStruxure ^a Control Expert, including all Unity Pro versions (former name of EcoStruxure ^a Control Expert, all versions), PLC Simulator for EcoStruxure ^a Process Expert including all HDCS versions (former name of EcoStruxure ^a Process Expert, all versions), Modicon Quantum CPU (part numbers 140CPU*, all versions), Modicon Premium CPU (part numbers TSXP5*, all versions). CVE ID : CVE-2021-22789		
	bounds	02-Sep-21	4	Read vulnerability that could cause a Denial of Service on the Modicon PLC controller / simulator when updating the controller application with a specially crafted project file exists in Modicon M580 CPU (part numbers BMEP* and BMEH*, all versions), Modicon M340 CPU (part numbers BMXP34*, all	load.schneide r- electric.com/f iles?p_Doc_Re f=SEVD-	

Page 780 of 1474

	 (part numbers BMKC80*, all versions), Modicon Momentum Ethernet CPU (part numbers 171CBU*, all versions), PLC Simulator for EcoStruxure^a Control Expert, including all Unity Pro versions (former name of EcoStruxure^a Control Expert, all versions), PLC Simulator for EcoStruxure^a Process Expert including all HDCS versions (former name of EcoStruxure^a Process Expert, all versions), Modicon Quantum CPU (part numbers 140CPU*, all versions), Modicon Premium CPU (part 		
	numbers TSXP5*, all versions). CVE ID : CVE-2021-22790		
Out-of- bounds 02-Sep-21 4 Write	A CWE-787: Out-of-bounds Write vulnerability that could cause a Denial of Service on the Modicon PLC controller / simulator when updating the controller application with a specially crafted project file exists in Modicon M580 CPU (part numbers BMEP* and BMEH*, all versions), Modicon M340 CPU (part numbers BMXP34*, all versions), Modicon MC80 (part numbers BMKC80*, all versions), Modicon Momentum Ethernet CPU (part numbers 171CBU*, all versions), PLC Simulator for EcoStruxure ^a Control Expert,	https://down load.schneide r- electric.com/f iles?p_Doc_Re f=SEVD- 2021-222-04	H-SCH-MODI- 180921/2041

Page 781 of 1474

NULL Pointer Dereference 02-Sep-21	ness Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Pointer 02-Sep-21			including all Unity Pro versions (former name of EcoStruxure ^a Control Expert, all versions), PLC Simulator for EcoStruxure ^a Process Expert including all HDCS versions (former name of EcoStruxure ^a Process Expert, all versions), Modicon Quantum CPU (part numbers 140CPU*, all versions), Modicon Premium CPU (part numbers TSXP5*, all versions). CVE ID : CVE-2021-22791		
		5	A CWE-476: NULL Pointer Dereference vulnerability that could cause a Denial of Service on the Modicon PLC controller / simulator when updating the controller application with a specially crafted project file exists in Modicon M580 CPU (part numbers BMEP* and BMEH*, all versions), Modicon M340 CPU (part numbers BMXP34*, all versions), Modicon MC80 (part numbers BMKC80*, all versions), Modicon Momentum Ethernet CPU (part numbers 171CBU*, all versions), PLC Simulator for EcoStruxure ^a Control Expert, including all Unity Pro versions (former name of EcoStruxure ^a Control Expert, all versions), PLC Simulator for EcoStruxure ^a Process	https://down load.schneide r- electric.com/f iles?p_Doc_Re f=SEVD- 2021-222-04	H-SCH-MODI- 180921/2042

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Expert including all HDCS versions (former name of EcoStruxure ^a Process Expert, all versions), Modicon Quantum CPU (part numbers 140CPU*, all versions), Modicon Premium CPU (part numbers TSXP5*, all versions). CVE ID : CVE-2021-22792		
modicon_mo	mentum_171	.cbu98			
Improper Restriction of Operations within the Bounds of a Memory Buffer	02-Sep-21	4	A CWE-119: Improper Restriction of Operations within the Bounds of a Memory Buffer vulnerability that could cause a Denial of Service on the Modicon PLC controller / simulator when updating the controller application with a specially crafted project file exists in Modicon M580 CPU (part numbers BMEP* and BMEH*, all versions), Modicon M340 CPU (part numbers BMXP34*, all versions), Modicon MC80 (part numbers BMKC80*, all versions), Modicon Momentum Ethernet CPU (part numbers 171CBU*, all versions), PLC Simulator for EcoStruxure ^a Control Expert, including all Unity Pro versions (former name of EcoStruxure ^a Control Expert, all versions), PLC Simulator for EcoStruxure ^a Process Expert including all HDCS	https://down load.schneide r- electric.com/f iles?p_Doc_Re f=SEVD- 2021-222-04	H-SCH-MODI- 180921/2043

CVSS Scoring Scale	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10
			р	aga 702 a	£1474					

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			versions (former name of EcoStruxure ^a Process Expert, all versions), Modicon Quantum CPU (part numbers 140CPU*, all versions), Modicon Premium CPU (part numbers TSXP5*, all versions). CVE ID : CVE-2021-22789		
Out-of- bounds Read	02-Sep-21	4	A CWE-125: Out-of-bounds Read vulnerability that could cause a Denial of Service on the Modicon PLC controller / simulator when updating the controller application with a specially crafted project file exists in Modicon M580 CPU (part numbers BMEP* and BMEH*, all versions), Modicon M340 CPU (part numbers BMXP34*, all versions), Modicon MC80 (part numbers BMKC80*, all versions), Modicon MC80 (part numbers BMKC80*, all versions), Modicon Momentum Ethernet CPU (part numbers 171CBU*, all versions), PLC Simulator for EcoStruxure ^a Control Expert, including all Unity Pro versions (former name of EcoStruxure ^a Control Expert, all versions), PLC Simulator for EcoStruxure ^a Process Expert including all HDCS versions (former name of EcoStruxure ^a Process Expert, all versions), Modicon Quantum CPU (part numbers 140CPU*, all versions), Modicon Premium CPU (part	https://down load.schneide r- electric.com/f iles?p_Doc_Re f=SEVD- 2021-222-04	H-SCH-MODI- 180921/2044
CVSS Scoring So	cale 0-1	1-2	2-3 3-4 4-5 5-6 Page 784 of 1474	6-7 7-8	8-9 9-10

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			numbers TSXP5*, all versions). CVE ID : CVE-2021-22790		
Out-of- bounds Write	02-Sep-21	4	A CWE-787: Out-of-bounds Write vulnerability that could cause a Denial of Service on the Modicon PLC controller / simulator when updating the controller application with a specially crafted project file exists in Modicon M580 CPU (part numbers BMEP* and BMEH*, all versions), Modicon M340 CPU (part numbers BMXP34*, all versions), Modicon MC80 (part numbers BMKC80*, all versions), Modicon Momentum Ethernet CPU (part numbers 171CBU*, all versions), PLC Simulator for EcoStruxure ^a Control Expert, including all Unity Pro versions (former name of EcoStruxure ^a Control Expert, all versions), PLC Simulator for EcoStruxure ^a Process Expert including all HDCS versions (former name of EcoStruxure ^a Process Expert, all versions), Modicon Quantum CPU (part numbers 140CPU*, all versions), Modicon Premium CPU (part numbers TSXP5*, all versions). CVE ID : CVE-2021-22791	https://down load.schneide r- electric.com/f iles?p_Doc_Re f=SEVD- 2021-222-04	H-SCH-MODI- 180921/2045
NULL Pointer	02-Sep-21	5	A CWE-476: NULL Pointer Dereference vulnerability	https://down load.schneide	H-SCH-MODI- 180921/2046

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Dereference			that could cause a Denial of Service on the Modicon PLC controller / simulator when updating the controller application with a specially crafted project file exists in Modicon M580 CPU (part numbers BMEP* and BMEH*, all versions), Modicon M340 CPU (part numbers BMXP34*, all versions), Modicon MC80 (part numbers BMKC80*, all versions), Modicon Momentum Ethernet CPU (part numbers 171CBU*, all versions), PLC Simulator for EcoStruxure ^a Control Expert, including all Unity Pro versions (former name of EcoStruxure ^a Control Expert, all versions), PLC Simulator for EcoStruxure ^a Process Expert including all HDCS versions (former name of EcoStruxure ^a Process Expert, all versions), Modicon Quantum CPU (part numbers 140CPU*, all versions), Modicon Premium CPU (part numbers TSXP5*, all versions).	r- electric.com/f iles?p_Doc_Re f=SEVD- 2021-222-04	
modicon_pre	mium tsxn5'	7 1634			
Improper			A CWE-119: Improper	https://down	
Restriction of Operations within the	Restriction of 02-Sep-21 4 Operations		Restriction of Operations within the Bounds of a Memory Buffer vulnerability that could cause a Denial of	load.schneide r- electric.com/f iles?p_Doc_Re	H-SCH-MODI- 180921/2047
CVSS Scoring Sc	ale 0-1	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
			P	age 786 o	f 1474					

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Bounds of a Memory Buffer			Service on the Modicon PLC controller / simulator when updating the controller application with a specially crafted project file exists in Modicon M580 CPU (part numbers BMEP* and BMEH*, all versions), Modicon M340 CPU (part numbers BMXP34*, all versions), Modicon MC80 (part numbers BMKC80*, all versions), Modicon Momentum Ethernet CPU (part numbers 171CBU*, all versions), PLC Simulator for EcoStruxure ^a Control Expert, including all Unity Pro versions (former name of EcoStruxure ^a Control Expert, all versions), PLC Simulator for EcoStruxure ^a Process Expert including all HDCS versions (former name of EcoStruxure ^a Process Expert, all versions), Modicon Quantum CPU (part numbers 140CPU*, all versions), Modicon Premium CPU (part numbers TSXP5*, all versions).	f=SEVD- 2021-222-04	
Out-of- bounds Read CVSS Scoring Sc	02-Sep-21	4	A CWE-125: Out-of-bounds Read vulnerability that could cause a Denial of Service on the Modicon PLC controller / simulator when updating the controller application with a specially crafted project file exists in Modicon M580 CPU 2-3 3-4 4-5 5-6	https://down load.schneide r- electric.com/f iles?p_Doc_Re f=SEVD- 2021-222-04	H-SCH-MODI- 180921/2048 8-9 9-10

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			(part numbers BMEP* and BMEH*, all versions), Modicon M340 CPU (part numbers BMXP34*, all versions), Modicon MC80 (part numbers BMKC80*, all versions), Modicon Momentum Ethernet CPU (part numbers 171CBU*, all versions), PLC Simulator for EcoStruxure ^a Control Expert, including all Unity Pro versions (former name of EcoStruxure ^a Control Expert, all versions), PLC Simulator for EcoStruxure ^a Process Expert including all HDCS versions (former name of EcoStruxure ^a Process Expert, all versions), Modicon Quantum CPU (part numbers 140CPU*, all versions), Modicon Premium CPU (part numbers TSXP5*, all versions).		
Out-of- bounds Write	02-Sep-21	4	A CWE-787: Out-of-bounds Write vulnerability that could cause a Denial of Service on the Modicon PLC controller / simulator when updating the controller application with a specially crafted project file exists in Modicon M580 CPU (part numbers BMEP* and BMEH*, all versions), Modicon M340 CPU (part numbers BMXP34*, all versions), Modicon MC80 (part numbers BMKC80*, all	https://down load.schneide r- electric.com/f iles?p_Doc_Re f=SEVD- 2021-222-04	H-SCH-MODI- 180921/2049
CVSS Scoring Sc	ale 0-1	1-2	2-3 3-4 4-5 5-6	6-7 7-8	8-9 9-10

			versions), Modicon		
			Momentum Ethernet CPU (part numbers 171CBU*, all versions), PLC Simulator for EcoStruxure ^a Control Expert, including all Unity Pro versions (former name of EcoStruxure ^a Control Expert, all versions), PLC Simulator for EcoStruxure ^a Process Expert including all HDCS versions (former name of EcoStruxure ^a Process Expert, all versions), Modicon Quantum CPU (part numbers 140CPU*, all versions), Modicon Premium CPU (part numbers TSXP5*, all versions). CVE ID : CVE-2021-22791		
NULL Pointer Dereference	02-Sep-21	5	A CWE-476: NULL Pointer Dereference vulnerability that could cause a Denial of Service on the Modicon PLC controller / simulator when updating the controller application with a specially crafted project file exists in Modicon M580 CPU (part numbers BMEP* and BMEH*, all versions), Modicon M340 CPU (part numbers BMXP34*, all versions), Modicon MC80 (part numbers BMKC80*, all versions), Modicon Momentum Ethernet CPU (part numbers 171CBU*, all versions), PLC Simulator for EcoStruxure ^a Control Expert,	https://down load.schneide r- electric.com/f iles?p_Doc_Re f=SEVD- 2021-222-04	H-SCH-MODI- 180921/2050

Page 789 of 1474

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			including all Unity Pro versions (former name of EcoStruxure ^a Control Expert, all versions), PLC Simulator for EcoStruxure ^a Process Expert including all HDCS versions (former name of EcoStruxure ^a Process Expert, all versions), Modicon Quantum CPU (part numbers 140CPU*, all versions), Modicon Premium CPU (part numbers TSXP5*, all versions). CVE ID : CVE-2021-22792		
modicon_pre	emium_tsxp5'	7_2634	m		
Improper Restriction of Operations within the Bounds of a Memory Buffer	02-Sep-21	4	A CWE-119: Improper Restriction of Operations within the Bounds of a Memory Buffer vulnerability that could cause a Denial of Service on the Modicon PLC controller / simulator when updating the controller application with a specially crafted project file exists in Modicon M580 CPU (part numbers BMEP* and BMEH*, all versions), Modicon M340 CPU (part numbers BMXP34*, all versions), Modicon MC80 (part numbers BMKC80*, all versions), Modicon Momentum Ethernet CPU (part numbers 171CBU*, all versions), PLC Simulator for EcoStruxure ^a Control Expert, including all Unity Pro	https://down load.schneide r- electric.com/f iles?p_Doc_Re f=SEVD- 2021-222-04	H-SCH-MODI- 180921/2051

CVSS Scoring Scale	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10
			D	200 700 0	f 1/7/					

			versions (former name of EcoStruxure ^a Control Expert, all versions), PLC Simulator for EcoStruxure ^a Process Expert including all HDCS versions (former name of EcoStruxure ^a Process Expert, all versions), Modicon Quantum CPU (part numbers 140CPU*, all versions), Modicon Premium CPU (part numbers TSXP5*, all versions). CVE ID : CVE-2021-22789		
Out-of- bounds Read	02-Sep-21	4	A CWE-125: Out-of-bounds Read vulnerability that could cause a Denial of Service on the Modicon PLC controller / simulator when updating the controller application with a specially crafted project file exists in Modicon M580 CPU (part numbers BMEP* and BMEH*, all versions), Modicon M340 CPU (part numbers BMXP34*, all versions), Modicon MC80 (part numbers BMKC80*, all versions), Modicon Momentum Ethernet CPU (part numbers 171CBU*, all versions), PLC Simulator for EcoStruxure ^a Control Expert, including all Unity Pro versions (former name of EcoStruxure ^a Process Expert including all HDCS versions (former name of	https://down load.schneide r- electric.com/f iles?p_Doc_Re f=SEVD- 2021-222-04	H-SCH-MODI- 180921/2052

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			EcoStruxure ^a Process Expert, all versions), Modicon Quantum CPU (part numbers 140CPU*, all versions), Modicon Premium CPU (part numbers TSXP5*, all versions).		
			CVE ID : CVE-2021-22790 A CWE-787: Out-of-bounds		
Out-of- bounds Write	02-Sep-21	4	Write vulnerability that could cause a Denial of Service on the Modicon PLC controller / simulator when updating the controller application with a specially crafted project file exists in Modicon M580 CPU (part numbers BMEP* and BMEH*, all versions), Modicon M340 CPU (part numbers BMXP34*, all versions), Modicon MC80 (part numbers BMKC80*, all versions), Modicon Momentum Ethernet CPU (part numbers 171CBU*, all versions), PLC Simulator for EcoStruxure ^a Control Expert, including all Unity Pro versions (former name of EcoStruxure ^a Control Expert, all versions), PLC Simulator for EcoStruxure ^a Process Expert including all HDCS versions (former name of EcoStruxure ^a Process Expert, all versions), Modicon Quantum CPU (part numbers 140CPU*, all versions), Modicon Premium CPU (part numbers TSXP5*, all	https://down load.schneide r- electric.com/f iles?p_Doc_Re f=SEVD- 2021-222-04	H-SCH-MODI- 180921/2053
CVSS Scoring Sc	ale 0-1	1-2	2-3 3-4 4-5 5-6	6-7 7-8	8-9 9-10

		versions).		
		,		
		CVE ID : CVE-2021-22791		
NULL Pointer Dereference	p-21 5	A CWE-476: NULL Pointer Dereference vulnerability that could cause a Denial of Service on the Modicon PLC controller / simulator when updating the controller application with a specially crafted project file exists in Modicon M580 CPU (part numbers BMEP* and BMEH*, all versions), Modicon M340 CPU (part numbers BMXP34*, all versions), Modicon MC80 (part numbers BMKC80*, all versions), Modicon Momentum Ethernet CPU (part numbers 171CBU*, all versions), PLC Simulator for EcoStruxure ^a Control Expert, including all Unity Pro versions (former name of EcoStruxure ^a Control Expert, all versions), PLC Simulator for EcoStruxure ^a Process Expert including all HDCS versions (former name of EcoStruxure ^a Process Expert, all versions), Modicon Quantum CPU (part numbers 140CPU*, all versions), Modicon Premium CPU (part numbers TSXP5*, all versions). CVE ID : CVE-2021-22792	https://down load.schneide r- electric.com/f iles?p_Doc_Re f=SEVD- 2021-222-04	H-SCH-MODI- 180921/2054

CVSS Scoring Scale	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10
			D	200 793 0	f 1/7/					

Improper Restriction of Operations within the Bounds of a Memory Buffer vulnerability that could cause a Denial of Service on the Modicon PLC controller / simulator when updating the controller application with a specially crafted project file exists in Modicon M580 CPU (part numbers BMEP* and BMEH*, all versions), Modicon M580 CPU (part numbers BMK280*, all versions), PLC Simulator for EcoStruxure ^a Control Expert, all versions), PLC Simulator for EcoStruxure ^a Control Expert, all versions), Modicon quantum CPU (part numbers 140CPI*, all versions), Modicon Pure unembers TSXP5*, all versions). CVEID : CVE-2021-22789H-SCH-MODI- lis?p_Doc_Re f=SEVD- 201-222-04Out-of- bounds02-Sep-214A CWE-125: Out-of-bounds Read vulnerability that could case a Denial of Service on load.schneide r-Out-of- bounds02-Sep-214A CWE-125: Out-of-bounds Read vulnerability that could case a Denial of Service on load.schneide r-	Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Out-of- bounds 02-Sep-21 4 Read vulnerability that could load.schneide 180921/2056	Restriction of Operations within the Bounds of a Memory	02-Sep-21	4	Restriction of Operations within the Bounds of a Memory Buffer vulnerability that could cause a Denial of Service on the Modicon PLC controller / simulator when updating the controller application with a specially crafted project file exists in Modicon M580 CPU (part numbers BMEP* and BMEH*, all versions), Modicon M340 CPU (part numbers BMXP34*, all versions), Modicon MC80 (part numbers BMKC80*, all versions), Modicon Momentum Ethernet CPU (part numbers 171CBU*, all versions), PLC Simulator for EcoStruxure ^a Control Expert, including all Unity Pro versions (former name of EcoStruxure ^a Control Expert, all versions), PLC Simulator for EcoStruxure ^a Process Expert including all HDCS versions (former name of EcoStruxure ^a Process Expert, all versions), Modicon Quantum CPU (part numbers 140CPU*, all versions), Modicon Premium CPU (part numbers TSXP5*, all versions).	load.schneide r- electric.com/f iles?p_Doc_Re f=SEVD-	
		02-Sep-21	4	Read vulnerability that could	load.schneide	

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Read			the Modicon PLC controller / simulator when updating the controller application with a specially crafted project file exists in Modicon M580 CPU (part numbers BMEP* and BMEH*, all versions), Modicon M340 CPU (part numbers BMXP34*, all versions), Modicon MC80 (part numbers BMKC80*, all versions), Modicon MC80 (part numbers BMKC80*, all versions), Modicon Momentum Ethernet CPU (part numbers 171CBU*, all versions), PLC Simulator for EcoStruxure ^a Control Expert, including all Unity Pro versions (former name of EcoStruxure ^a Control Expert, all versions), PLC Simulator for EcoStruxure ^a Process Expert including all HDCS versions (former name of EcoStruxure ^a Process Expert, all versions), Modicon Quantum CPU (part numbers 140CPU*, all versions), Modicon Premium CPU (part numbers TSXP5*, all versions). CVE ID : CVE-2021-22790	electric.com/f iles?p_Doc_Re f=SEVD- 2021-222-04	
Out-of- bounds Write CVSS Scoring Sc	02-Sep-21 ale 0-1	4	A CWE-787: Out-of-bounds Write vulnerability that could cause a Denial of Service on the Modicon PLC controller / simulator when updating the controller application with a specially crafted project file exists in Modicon M580 CPU (part numbers BMEP* and 2-3 3-4 4-5 5-6	https://down load.schneide r- electric.com/f iles?p_Doc_Re f=SEVD- 2021-222-04	H-SCH-MODI- 180921/2057 8-9 9-10

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			BMEH*, all versions), Modicon M340 CPU (part numbers BMXP34*, all versions), Modicon MC80 (part numbers BMKC80*, all versions), Modicon Momentum Ethernet CPU (part numbers 171CBU*, all versions), PLC Simulator for EcoStruxure ^a Control Expert, including all Unity Pro versions (former name of EcoStruxure ^a Control Expert, all versions), PLC Simulator for EcoStruxure ^a Process Expert including all HDCS versions (former name of EcoStruxure ^a Process Expert, all versions), Modicon Quantum CPU (part numbers 140CPU*, all versions), Modicon Premium CPU (part numbers TSXP5*, all versions).		
NULL Pointer Dereference	02-Sep-21	5	A CWE-476: NULL Pointer Dereference vulnerability that could cause a Denial of Service on the Modicon PLC controller / simulator when updating the controller application with a specially crafted project file exists in Modicon M580 CPU (part numbers BMEP* and BMEH*, all versions), Modicon M340 CPU (part numbers BMXP34*, all versions), Modicon MC80 (part numbers BMKC80*, all	https://down load.schneide r- electric.com/f iles?p_Doc_Re f=SEVD- 2021-222-04	H-SCH-MODI- 180921/2058
CVSS Scoring Sc	ale 0-1	1-2	2-3 3-4 4-5 5-6	6-7 7-8	8-9 9-10

Page 796 of 1474

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			versions), Modicon Momentum Ethernet CPU (part numbers 171CBU*, all versions), PLC Simulator for EcoStruxure ^a Control Expert, including all Unity Pro versions (former name of EcoStruxure ^a Control Expert, all versions), PLC Simulator for EcoStruxure ^a Process Expert including all HDCS versions (former name of EcoStruxure ^a Process Expert, all versions), Modicon Quantum CPU (part numbers 140CPU*, all versions), Modicon Premium CPU (part numbers TSXP5*, all versions).		
modicon_pre	emium_tsxp57	7_454n	n		
Improper Restriction of Operations within the Bounds of a Memory Buffer	02-Sep-21	4	A CWE-119: Improper Restriction of Operations within the Bounds of a Memory Buffer vulnerability that could cause a Denial of Service on the Modicon PLC controller / simulator when updating the controller application with a specially crafted project file exists in Modicon M580 CPU (part numbers BMEP* and BMEH*, all versions), Modicon M340 CPU (part numbers BMXP34*, all versions), Modicon MC80 (part numbers BMKC80*, all versions), Modicon	https://down load.schneide r- electric.com/f iles?p_Doc_Re f=SEVD- 2021-222-04	H-SCH-MODI- 180921/2059

CVSS Scoring Scale	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10
Dago 707 of 1474										

bounds 02-Sep-21 4 Modicon M240 CDU (nort electric com/f	Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Out-of- bounds02-Sep-214Read vulnerability that could cause a Denial of Service on the Modicon PLC controller / simulator when updating the controller application with a specially crafted project file exists in Modicon M580 CPU BMEH*, all versions), Modicon M340 CPU (part numbers BMXP34*, all versions), Modicon MC80 (part numbers BMKC80*, all versions), Modicon Momentum Ethernet CPU (part numbers 171CBU*, all versions), PLC Simulator forH-SCH-M H-SCH-M 180921/ H-SCH-M 2021-222-04				(part numbers 171CBU*, all versions), PLC Simulator for EcoStruxure ^a Control Expert, including all Unity Pro versions (former name of EcoStruxure ^a Control Expert, all versions), PLC Simulator for EcoStruxure ^a Process Expert including all HDCS versions (former name of EcoStruxure ^a Process Expert, all versions), Modicon Quantum CPU (part numbers 140CPU*, all versions), Modicon Premium CPU (part numbers TSXP5*, all versions).		
including all Unity Proversions (former name of CVSS Scoring Scale 0-1 1-2 2-3 3-4 4-5 5-6 6-7 7-8 8-9	ounds Read			Read vulnerability that could cause a Denial of Service on the Modicon PLC controller / simulator when updating the controller application with a specially crafted project file exists in Modicon M580 CPU (part numbers BMEP* and BMEH*, all versions), Modicon M340 CPU (part numbers BMXP34*, all versions), Modicon MC80 (part numbers BMKC80*, all versions), Modicon Momentum Ethernet CPU (part numbers 171CBU*, all versions), PLC Simulator for EcoStruxure ^a Control Expert, including all Unity Pro versions (former name of	load.schneide r- electric.com/f iles?p_Doc_Re f=SEVD- 2021-222-04	H-SCH-MODI- 180921/2060

Out-of- bounds 02-Sep-21 4	Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Out-of- 02-Sep-21 4 A CWE-787: Out-of-bounds Nrite vulnerability that could Nrite vulnerability that could Out-of- ismulator when updating the cause a Denial of Service on HAGMCON MS80 CPU HAGMCON MS80 CPU Write vulnerability that exists in Modicon MS80 CPU (part numbers BMEP* and BMEH*, all versions), HAGMCON MS80 HAGMCON MS80 Write 02-Sep-21 4 (part numbers BMKP34*, all load.schneide H-SCH-MODI- Write versions), Modicon MC80 r- H-SCH-MODI- (part numbers BMKP34*, all load.schneide H-SCH-MODI- (part numbers BMKC80*, all electric.com/f 180921/2061 (part numbers 171CBU*, all 2021-222-04 H-SCH-MODI- (part numbers 171CBU*, all ilcum/f H-SCH-MODI- (part numbers 171CBU*, all 2021-222-04 H-SCH-MODI- (part numbers 171CBU*, all ilcum/f H-SCH-MODI- (part numbers 171CBU*, all ilcum/f <td></td> <td></td> <td></td> <td>all versions), PLC Simulator for EcoStruxure^ª Process Expert including all HDCS versions (former name of EcoStruxure^ª Process Expert, all versions), Modicon Quantum CPU (part numbers 140CPU*, all versions), Modicon Premium CPU (part numbers TSXP5*, all versions).</td> <td></td> <td></td>				all versions), PLC Simulator for EcoStruxure ^ª Process Expert including all HDCS versions (former name of EcoStruxure ^ª Process Expert, all versions), Modicon Quantum CPU (part numbers 140CPU*, all versions), Modicon Premium CPU (part numbers TSXP5*, all versions).		
	bounds Write			A CWE-787: Out-of-bounds Write vulnerability that could cause a Denial of Service on the Modicon PLC controller / simulator when updating the controller application with a specially crafted project file exists in Modicon M580 CPU (part numbers BMEP* and BMEH*, all versions), Modicon M340 CPU (part numbers BMXP34*, all versions), Modicon MC80 (part numbers BMKC80*, all versions), Modicon MC80 (part numbers BMKC80*, all versions), Modicon Momentum Ethernet CPU (part numbers 171CBU*, all versions), PLC Simulator for EcoStruxure ^a Control Expert, including all Unity Pro versions (former name of EcoStruxure ^a Control Expert, all versions), PLC Simulator for EcoStruxure ^a Process Expert including all HDCS versions (former name of	load.schneide r- electric.com/f iles?p_Doc_Re f=SEVD- 2021-222-04	180921/2061

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			all versions), Modicon Quantum CPU (part numbers 140CPU*, all versions), Modicon Premium CPU (part numbers TSXP5*, all versions).		
			CVE ID : CVE-2021-22791		
NULL Pointer Dereference	02-Sep-21	5	A CWE-476: NULL Pointer Dereference vulnerability that could cause a Denial of Service on the Modicon PLC controller / simulator when updating the controller application with a specially crafted project file exists in Modicon M580 CPU (part numbers BMEP* and BMEH*, all versions), Modicon M340 CPU (part numbers BMXP34*, all versions), Modicon MC80 (part numbers BMKC80*, all versions), Modicon Momentum Ethernet CPU (part numbers 171CBU*, all versions), PLC Simulator for EcoStruxure ^a Control Expert, including all Unity Pro versions (former name of EcoStruxure ^a Control Expert, all versions), PLC Simulator for EcoStruxure ^a Process Expert including all HDCS versions (former name of EcoStruxure ^a Process Expert, all versions), Modicon Quantum CPU (part numbers 140CPU*, all versions), Modicon Premium CPU (part numbers TSXP5*, all	https://down load.schneide r- electric.com/f iles?p_Doc_Re f=SEVD- 2021-222-04	H-SCH-MODI- 180921/2062
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 & CVE ID	Patch	NCIIPC ID
			versions).		
			CVE ID : CVE-2021-22792		
modicon_pre	emium_tsxp5'	7_4634	m		
Improper Restriction of Operations within the Bounds of a Memory Buffer	02-Sep-21	4	A CWE-119: Improper Restriction of Operations within the Bounds of a Memory Buffer vulnerability that could cause a Denial of Service on the Modicon PLC controller / simulator when updating the controller application with a specially crafted project file exists in Modicon M580 CPU (part numbers BMEP* and BMEH*, all versions), Modicon M340 CPU (part numbers BMXP34*, all versions), Modicon MC80 (part numbers BMKC80*, all versions), Modicon Momentum Ethernet CPU (part numbers 171CBU*, all versions), PLC Simulator for EcoStruxure ^a Control Expert, including all Unity Pro versions (former name of EcoStruxure ^a Control Expert, all versions), PLC Simulator for EcoStruxure ^a Process Expert including all HDCS versions (former name of EcoStruxure ^a Process Expert, all versions), Modicon Quantum CPU (part numbers 140CPU*, all versions), Modicon Premium CPU (part numbers TSXP5*, all versions).	https://down load.schneide r- electric.com/f iles?p_Doc_Re f=SEVD- 2021-222-04	H-SCH-MODI- 180921/2063

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2021-22789		
Out-of- bounds Read	02-Sep-21	4	A CWE-125: Out-of-bounds Read vulnerability that could cause a Denial of Service on the Modicon PLC controller / simulator when updating the controller application with a specially crafted project file exists in Modicon M580 CPU (part numbers BMEP* and BMEH*, all versions), Modicon M340 CPU (part numbers BMXP34*, all versions), Modicon MC80 (part numbers BMKC80*, all versions), Modicon Momentum Ethernet CPU (part numbers 171CBU*, all versions), PLC Simulator for EcoStruxure ^a Control Expert, including all Unity Pro versions (former name of EcoStruxure ^a Control Expert, all versions), PLC Simulator for EcoStruxure ^a Process Expert including all HDCS versions (former name of EcoStruxure ^a Process Expert, all versions), Modicon Quantum CPU (part numbers 140CPU*, all versions), Modicon Premium CPU (part numbers TSXP5*, all versions). CVE ID : CVE-2021-22790	https://down load.schneide r- electric.com/f iles?p_Doc_Re f=SEVD- 2021-222-04	H-SCH-MODI- 180921/2064
Out-of- bounds Write	02-Sep-21	4	A CWE-787: Out-of-bounds Write vulnerability that could cause a Denial of Service on the Modicon PLC controller /	https://down load.schneide r- electric.com/f	H-SCH-MODI- 180921/2065

CVSS Scoring Scale	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10
			D		£1171					

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			simulator when updating the controller application with a specially crafted project file exists in Modicon M580 CPU (part numbers BMEP* and BMEH*, all versions), Modicon M340 CPU (part numbers BMXP34*, all versions), Modicon MC80 (part numbers BMKC80*, all versions), Modicon MC80 (part numbers BMKC80*, all versions), Modicon Momentum Ethernet CPU (part numbers 171CBU*, all versions), PLC Simulator for EcoStruxure ^a Control Expert, including all Unity Pro versions (former name of EcoStruxure ^a Control Expert, all versions), PLC Simulator for EcoStruxure ^a Process Expert including all HDCS versions (former name of EcoStruxure ^a Process Expert, all versions), Modicon Quantum CPU (part numbers 140CPU*, all versions), Modicon Premium CPU (part numbers TSXP5*, all versions).	iles?p_Doc_Re f=SEVD- 2021-222-04	
NULL Pointer Dereference CVSS Scoring Sc	02-Sep-21	5	A CWE-476: NULL Pointer Dereference vulnerability that could cause a Denial of Service on the Modicon PLC controller / simulator when updating the controller application with a specially crafted project file exists in Modicon M580 CPU (part numbers BMEP* and BMEH*,	https://down load.schneide r- electric.com/f iles?p_Doc_Re f=SEVD- 2021-222-04	H-SCH-MODI- 180921/2066

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			all versions), Modicon M340 CPU (part numbers BMXP34*, all versions), Modicon MC80 (part numbers BMKC80*, all versions), Modicon Momentum Ethernet CPU (part numbers 171CBU*, all versions), PLC Simulator for EcoStruxure ^a Control Expert, including all Unity Pro versions (former name of EcoStruxure ^a Control Expert, all versions), PLC Simulator for EcoStruxure ^a Process Expert including all HDCS versions (former name of EcoStruxure ^a Process Expert, all versions), Modicon Quantum CPU (part numbers 140CPU*, all versions), Modicon Premium CPU (part numbers TSXP5*, all versions). CVE ID : CVE-2021-22792		
modicon pre	mium texn5'	7 554n			
Improper Restriction of Operations within the Bounds of a Memory Buffer	02-Sep-21	4	A CWE-119: Improper Restriction of Operations within the Bounds of a Memory Buffer vulnerability that could cause a Denial of Service on the Modicon PLC controller / simulator when updating the controller application with a specially crafted project file exists in Modicon M580 CPU (part numbers BMEP* and BMEH*, all versions), Modicon M340	https://down load.schneide r- electric.com/f iles?p_Doc_Re f=SEVD- 2021-222-04	H-SCH-MODI- 180921/2067

CVSS Scoring Scale	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10
			D	200 001 0	f 1 / 7 /					

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			CPU (part numbers BMXP34*, all versions), Modicon MC80 (part numbers BMKC80*, all versions), Modicon Momentum Ethernet CPU (part numbers 171CBU*, all versions), PLC Simulator for EcoStruxure ^a Control Expert, including all Unity Pro versions (former name of EcoStruxure ^a Control Expert, all versions), PLC Simulator for EcoStruxure ^a Process Expert including all HDCS versions (former name of EcoStruxure ^a Process Expert, all versions), Modicon Quantum CPU (part numbers 140CPU*, all versions), Modicon Premium CPU (part numbers TSXP5*, all versions).		
Out-of- bounds Read	02-Sep-21	4	A CWE-125: Out-of-bounds Read vulnerability that could cause a Denial of Service on the Modicon PLC controller / simulator when updating the controller application with a specially crafted project file exists in Modicon M580 CPU (part numbers BMEP* and BMEH*, all versions), Modicon M340 CPU (part numbers BMXP34*, all versions), Modicon MC80 (part numbers BMKC80*, all versions), Modicon	https://down load.schneide r- electric.com/f iles?p_Doc_Re f=SEVD- 2021-222-04	H-SCH-MODI- 180921/2068
CVSS Scoring Sc	ale 0-1	1-2	2-3 3-4 4-5 5-6	6-7 7-8	8-9 9-10

Out-of- bounds 02-Sep-21 4 (part numbers 171CBU*, all versions), PLC Simulator for EcoStruxure ^a Control Expert, all versions), PLC Simulator for EcoStruxure ^a Process Expert including all HDCS versions (former name of EcoStruxure ^a Process Expert, all versions), Modicon Quantum CPU (part numbers 140CPU*, all versions), Modicon Premium CPU (part numbers TSXP5*, all versions). • CVE ID : CVE-2021-22790 • A CWE-787: Out-of-bounds Write • 02-Sep-21 4 Modicon M580 CPU (part numbers BMEP* and BMEH*, all versions), Modicon M580 CPU (part numbers BMEP* and BMEH*, all versions), Modicon M580 CPU (part numbers BMEP* and BMEH*, all versions), Modicon M600 CPU (part numbers BMEP* and BMEH*, all versions), Modicon M600 CPU (part numbers BMEP* and BMEH*, all versions), Modicon M600 (part numbers BMEP* and BMEH*, all versions), Modicon M600 (part numbers BMEP* and BMEH*, all versions), Modicon M600 (part numbers BMEP* and Versions), Modicon MC80 (part numbers BMECB*, all versions), Modicon MC80 (part numbers METCB*, all versions), Modicon MC80 (part numbers Control Expert, including all Unity Pro versions (former name of EcoStruxure ^a Control Expert, including all Unity Pro Versions Versio	Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Out-of- bounds02-Sep-21ANeite vulnerability that could cause a Denial of Service on the Modicon PLC controller / simulator when updating the controller application with a specially crafted project file exists in Modicon M580 CPU (part numbers BMEP* and BMEH*, all versions), Nodicon M340 CPU (part lest), Modicon M340 CPU (part ersions), Modicon MC800 (part numbers BMXP34*, all versions), Modicon MC800 (part numbers BMKC80*, all) (part numbers 171CBU*, all) versions), PLC Simulator for EcoStruxure ^a Control Expert, including all Unity Pro versions (former name of EcoStruxure ^a Control Expert, including all Unity ProH-SCH-MODI- 180921/2069				versions), PLC Simulator for EcoStruxure ^a Control Expert, including all Unity Pro versions (former name of EcoStruxure ^a Control Expert, all versions), PLC Simulator for EcoStruxure ^a Process Expert including all HDCS versions (former name of EcoStruxure ^a Process Expert, all versions), Modicon Quantum CPU (part numbers 140CPU*, all versions), Modicon Premium CPU (part numbers TSXP5*, all versions).		
	bounds Write		4	A CWE-787: Out-of-bounds Write vulnerability that could cause a Denial of Service on the Modicon PLC controller / simulator when updating the controller application with a specially crafted project file exists in Modicon M580 CPU (part numbers BMEP* and BMEH*, all versions), Modicon M340 CPU (part numbers BMXP34*, all versions), Modicon MC80 (part numbers BMKC80*, all versions), Modicon Momentum Ethernet CPU (part numbers 171CBU*, all versions), PLC Simulator for EcoStruxure ^a Control Expert, including all Unity Pro versions (former name of EcoStruxure ^a Control Expert,	load.schneide r- electric.com/f iles?p_Doc_Re f=SEVD- 2021-222-04	

Page 806 of 1474

NULL Pointer Dereference02-Sep-215A A Septentional and the controller application with a specially controller specific part numbers application with a specially controller specific part numbers project file exists in Modicon MCB0 (Put part numbers BME0* and BMEH*, all versions), Modicon MCB0 (Put part numbers BME0* and BMEH*, all versions), Modicon MCB0 (part numbers BME0*, all versions), Modicon MCB0 (part numbers BME0*, all versions), PLC Simulator for EcoStruxure* Control Expert, all versions), PLC Simulator for EcoStruxure* Control Expert, all versions), PLC Simulator for EcoStruxure* Process Expert including all HDCS versions (former name of EcoStruxure* Process Expert including all HDCS versions (former name of <br< th=""><th>Weakness</th><th>Publish Date</th><th>CVSS</th><th>Description & CVE ID</th><th>Patch</th><th>NCIIPC ID</th></br<>	Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
NULL Pointer DereferenceA CWE-476: NULL Pointer Dereference vulnerability that could cause a Denial of Service on the Modicon PLC controller / simulator when updating the controller application with a specially crafted project file exists in Modicon M580 CPU (part numbers BMEP* and BMEH*, all versions), Modicon M340 CPU (part numbers BMXP34*, all versions), Modicon M680 (part numbers BMKC80*, all iles?p_Doc_Re f=SEVD- 2021-222-04H-SCH-MODI- 180921/2070NULL Pointer Dereference5Modicon MC80 (part numbers BMKC80*, all versions), Modicon (part numbers 171CBU*, all versions), PLC Simulator for EcoStruxureª Control Expert, including all Unity Pro versions (former name of EcoStruxureª Process Expert including all HDCS versions (former name of EcoStruxureª Process Expert including all HDCS versions (former name of EcoStruxureª Process Expert, all versions (former name of EcoStruxureª Process Expert,H-SCH-MODI- iles?p_Doc_Re f=SEVD- 2021-222-04				for EcoStruxure ^a Process Expert including all HDCS versions (former name of EcoStruxure ^a Process Expert, all versions), Modicon Quantum CPU (part numbers 140CPU*, all versions), Modicon Premium CPU (part numbers TSXP5*, all versions).		
NULL 02-Sep-21 5 Bereference vulnerability Hat could cause a Denial of Service on the Modicon PLC Hat could cause a Denial of Service on the Modicon PLC Hat could cause a Denial of Service on the Modicon PLC Hat could cause a Denial of Service on the Modicon PLC Hat could cause a Denial of Service on the Modicon PLC Hat could cause a Denial of Service on the Modicon PLC Hat could cause a Denial of Service on the Modicon PLC Hat could cause a Denial of Service on the Modicon PLC Hat could cause a Denial of Service on the Modicon PLC Hat could cause a Denial of Service on the Modicon PLC Hat could cause a Denial of Service on the Modicon PLC Hat could cause a Denial of Courding the controller Hat could cause a Denial of CPU (part numbers BMEP* and BMEH*; all versions), Modicon M380 (part Nodicon MC80 (part Nomentum Ethernet CPU (part numbers BMKC80*, all HescPI-Doc Re Versions), PLC Simulator H-SCH-MODI- 180921/2070 180921/2070 HescPI-Doc Re (part numbers 171CBU*, all Versions), PLC Simulator HescPI-Doc Re FesEVD- 2021-222-04 HescH-MODI- 180921/2070 180921/2070 HescPI-Doc Re (part numbers 171CBU*, all Versions), PLC Simulator HescH-MODI- 180921/2070 18040 Hesc Hesc Struxure ^a Control Expert, all versions), PLC Simulator Hesc Hesc Hesc Struxure ^a Process Expert including all HDCS Hesc Hesc Hesc Struxure ^a Process Expert including all HDCS Hesc Hesc Hesc Struxure ^a Process Expert including all HDCS Hesc Hesc Hesc Hesc Struxure ^a Pr						
	Pointer	02-Sep-21	5	Dereference vulnerability that could cause a Denial of Service on the Modicon PLC controller / simulator when updating the controller application with a specially crafted project file exists in Modicon M580 CPU (part numbers BMEP* and BMEH*, all versions), Modicon M340 CPU (part numbers BMXP34*, all versions), Modicon MC80 (part numbers BMKC80*, all versions), Modicon Momentum Ethernet CPU (part numbers 171CBU*, all versions), PLC Simulator for EcoStruxure ^a Control Expert, including all Unity Pro versions (former name of EcoStruxure ^a Control Expert, all versions), PLC Simulator for EcoStruxure ^a Process Expert including all HDCS versions (former name of	load.schneide r- electric.com/f iles?p_Doc_Re f=SEVD-	

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			all versions), Modicon Quantum CPU (part numbers 140CPU*, all versions), Modicon Premium CPU (part numbers TSXP5*, all versions). CVE ID : CVE-2021-22792		
modicon_pre	emium_tsxp5'	7_5634	m		
Improper Restriction of Operations within the Bounds of a Memory Buffer	02-Sep-21	4	A CWE-119: Improper Restriction of Operations within the Bounds of a Memory Buffer vulnerability that could cause a Denial of Service on the Modicon PLC controller / simulator when updating the controller application with a specially crafted project file exists in Modicon M580 CPU (part numbers BMEP* and BMEH*, all versions), Modicon M340 CPU (part numbers BMXP34*, all versions), Modicon MC80 (part numbers BMKC80*, all versions), Modicon Momentum Ethernet CPU (part numbers 171CBU*, all versions), PLC Simulator for EcoStruxure ^a Control Expert, including all Unity Pro versions (former name of EcoStruxure ^a Control Expert, all versions), PLC Simulator for EcoStruxure ^a Process Expert including all HDCS versions (former name of EcoStruxure ^a Process Expert, all versions), Modicon	https://down load.schneide r- electric.com/f iles?p_Doc_Re f=SEVD- 2021-222-04	H-SCH-MODI- 180921/2071

CVSS Scoring Scale	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10
0								- The second		
			D	aga 000 g	f 1 / 7 /					

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Quantum CPU (part numbers 140CPU*, all versions), Modicon Premium CPU (part numbers TSXP5*, all versions). CVE ID : CVE-2021-22789		
Out-of- bounds Read	02-Sep-21	4	A CWE-125: Out-of-bounds Read vulnerability that could cause a Denial of Service on the Modicon PLC controller / simulator when updating the controller application with a specially crafted project file exists in Modicon M580 CPU (part numbers BMEP* and BMEH*, all versions), Modicon M340 CPU (part numbers BMXP34*, all versions), Modicon MC80 (part numbers BMKC80*, all versions), Modicon Momentum Ethernet CPU (part numbers 171CBU*, all versions), PLC Simulator for EcoStruxure ^a Control Expert, including all Unity Pro versions (former name of EcoStruxure ^a Control Expert, all versions), PLC Simulator for EcoStruxure ^a Process Expert including all HDCS versions (former name of EcoStruxure ^a Process Expert, all versions), Modicon Quantum CPU (part numbers 140CPU*, all versions), Modicon Premium CPU (part numbers TSXP5*, all versions).	https://down load.schneide r- electric.com/f iles?p_Doc_Re f=SEVD- 2021-222-04	H-SCH-MODI- 180921/2072

CVSS Scoring Scale	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10
			Р	age 809 c	of 1474					

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2021-22790		
Out-of- bounds Write	02-Sep-21	4	A CWE-787: Out-of-bounds Write vulnerability that could cause a Denial of Service on the Modicon PLC controller / simulator when updating the controller application with a specially crafted project file exists in Modicon M580 CPU (part numbers BMEP* and BMEH*, all versions), Modicon M340 CPU (part numbers BMXP34*, all versions), Modicon MC80 (part numbers BMKC80*, all versions), Modicon Momentum Ethernet CPU (part numbers 171CBU*, all versions), PLC Simulator for EcoStruxure ^a Control Expert, including all Unity Pro versions (former name of EcoStruxure ^a Control Expert, all versions), PLC Simulator for EcoStruxure ^a Process Expert including all HDCS versions (former name of EcoStruxure ^a Process Expert, all versions), Modicon Quantum CPU (part numbers 140CPU*, all versions), Modicon Premium CPU (part numbers TSXP5*, all versions).	https://down load.schneide r- electric.com/f iles?p_Doc_Re f=SEVD- 2021-222-04	H-SCH-MODI- 180921/2073
NULL Pointer Dereference	02-Sep-21	5	A CWE-476: NULL Pointer Dereference vulnerability that could cause a Denial of Service on the Modicon PLC	https://down load.schneide r- electric.com/f	H-SCH-MODI- 180921/2074

CVSS Scoring Scale	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10
Dage 910 of 1474										

Page 810 of 1474

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID		
	on_premium_tsxp57_663		controller / simulator when updating the controller application with a specially crafted project file exists in Modicon M580 CPU (part numbers BMEP* and BMEH*, all versions), Modicon M340 CPU (part numbers BMXP34*, all versions), Modicon MC80 (part numbers BMKC80*, all versions), Modicon Momentum Ethernet CPU (part numbers 171CBU*, all versions), PLC Simulator for EcoStruxure ^a Control Expert, including all Unity Pro versions (former name of EcoStruxure ^a Control Expert, all versions), PLC Simulator for EcoStruxure ^a Process Expert including all HDCS versions (former name of EcoStruxure ^a Process Expert, all versions), Modicon Quantum CPU (part numbers 140CPU*, all versions), Modicon Premium CPU (part numbers TSXP5*, all versions).	iles?p_Doc_Re f=SEVD- 2021-222-04			
modicon_premium_tsxp57_6634m							
Improper Restriction of Operations within the Bounds of a Memory	02-Sep-21	4	A CWE-119: Improper Restriction of Operations within the Bounds of a Memory Buffer vulnerability that could cause a Denial of Service on the Modicon PLC controller / simulator when	https://down load.schneide r- electric.com/f iles?p_Doc_Re f=SEVD- 2021-222-04	H-SCH-MODI- 180921/2075		
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
Buffer			updating the controllerapplication with a speciallycrafted project file exists inModicon M580 CPU (partnumbers BMEP* and BMEH*,all versions), Modicon M340CPU (part numbersBMXP34*, all versions),Modicon MC80 (partnumbers BMKC80*, allversions), ModiconMomentum Ethernet CPU(part numbers 171CBU*, allversions), PLC Simulator forEcoStruxureª Control Expert,including all Unity Proversions (former name ofEcoStruxureª Control Expert,all versions), PLC Simulatorfor EcoStruxureª ProcessExpert including all HDCSversions (former name ofEcoStruxureª Process Expert,all versions), ModiconQuantum CPU (part numbers140CPU*, all versions),Modicon Premium CPU (partnumbers TSXP5*, allversions).CVE ID : CVE-2021-22789		
			A CWE-125: Out-of-bounds		
Out-of- bounds Read02-Sep-21444CVSS Scoring Scale0-10-11-2		Read vulnerability that could cause a Denial of Service on the Modicon PLC controller / simulator when updating the controller application with a specially crafted project file exists in Modicon M580 CPU (part numbers BMEP* and BMEH*, all versions),	https://down load.schneide r- electric.com/f iles?p_Doc_Re f=SEVD- 2021-222-04	H-SCH-MODI- 180921/2076	

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Modicon M340 CPU (part numbers BMXP34*, all versions), Modicon MC80 (part numbers BMKC80*, all versions), Modicon Momentum Ethernet CPU (part numbers 171CBU*, all versions), PLC Simulator for EcoStruxure ^a Control Expert, including all Unity Pro versions (former name of EcoStruxure ^a Control Expert, all versions), PLC Simulator for EcoStruxure ^a Process Expert including all HDCS versions (former name of EcoStruxure ^a Process Expert, all versions), Modicon Quantum CPU (part numbers 140CPU*, all versions), Modicon Premium CPU (part numbers TSXP5*, all versions). CVE ID : CVE-2021-22790		
Out-of- bounds Write	02-Sep-21	4	A CWE-787: Out-of-bounds Write vulnerability that could cause a Denial of Service on the Modicon PLC controller / simulator when updating the controller application with a specially crafted project file exists in Modicon M580 CPU (part numbers BMEP* and BMEH*, all versions), Modicon M340 CPU (part numbers BMXP34*, all versions), Modicon MC80 (part numbers BMKC80*, all versions), Modicon	https://down load.schneide r- electric.com/f iles?p_Doc_Re f=SEVD- 2021-222-04	H-SCH-MODI- 180921/2077
CVSS Scoring Sc	ale 0-1	1-2	2-3 3-4 4-5 5-6	6-7 7-8	8-9 9-10

NULL Pointer Dereference 02-Sep-21 5 5 CVE 10 CVE 10 CVE 10 RVE 3 Https://down load.schneide r. ecoStruxure ⁴ Control Expert, all versions), PLC Simulator for EcoStruxure ⁴ Process Expert including all HDCS versions (former name of EcoStruxure ⁴ Process Expert, all versions), Modicon Quantum CPU (part numbers 140C/Pt ⁺ , all versions), Modicon Premium CPU (part numbers TSXP5*, all versions). Https://down load.schneide r. electric.com/ft iles?p.Doc.Re FSEVD. NULL Pointer Dereference 02-Sep-21 5 KWE*476: NULL Pointer numbers BMEP* and BMEH*, all versions), Modicon MC80 (Put (part numbers BMEP* and BMEH*, all versions), Modicon MC80 (part numbers BMC80*, all versions), Modicon MC80 (part numbers MC80*, all versions), MO100 NULL PO10 NULL PO10 NULL PO10 V05550000 P0 P10 P2	Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
NULL Pointer Dereference02-Sep-215Dereference vulnerability that could cause a Denial of Service on the Modicon PLC controller / simulator when updating the controller application with a specially crafted project file exists in Ndoicon M580 CPU (part numbers BMEP* and BMEH*, all versions), Modicon M340 CPU (part numbers BMXP34*, all versions), Modicon MC80 (part numbers BMKC80*, all versions), Modicon Momentum Ethernet CPU (part numbers 171CBU*, all versions), PLC Simulator for EcoStruxureª Control Expert, including all Unity Pro versions (former name ofH-SCH-MODI- 180921/2078				versions), PLC Simulator for EcoStruxure ^a Control Expert, including all Unity Pro versions (former name of EcoStruxure ^a Control Expert, all versions), PLC Simulator for EcoStruxure ^a Process Expert including all HDCS versions (former name of EcoStruxure ^a Process Expert, all versions), Modicon Quantum CPU (part numbers 140CPU*, all versions), Modicon Premium CPU (part numbers TSXP5*, all versions).		
	Pointer	02-Sep-21	5	A CWE-476: NULL Pointer Dereference vulnerability that could cause a Denial of Service on the Modicon PLC controller / simulator when updating the controller application with a specially crafted project file exists in Modicon M580 CPU (part numbers BMEP* and BMEH*, all versions), Modicon M340 CPU (part numbers BMXP34*, all versions), Modicon MC80 (part numbers BMKC80*, all versions), Modicon Momentum Ethernet CPU (part numbers 171CBU*, all versions), PLC Simulator for EcoStruxure ^a Control Expert, including all Unity Pro	load.schneide r- electric.com/f iles?p_Doc_Re f=SEVD-	

Page 814 of 1474

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			EcoStruxure ^ª Control Expert, all versions), PLC Simulator for EcoStruxure ^ª Process Expert including all HDCS versions (former name of EcoStruxure ^ª Process Expert, all versions), Modicon Quantum CPU (part numbers 140CPU*, all versions), Modicon Premium CPU (part numbers TSXP5*, all versions). CVE ID : CVE-2021-22792		
modicon_qua	antum_140cp	u6515	0		
Improper Restriction of Operations within the Bounds of a Memory Buffer	02-Sep-21	4	A CWE-119: Improper Restriction of Operations within the Bounds of a Memory Buffer vulnerability that could cause a Denial of Service on the Modicon PLC controller / simulator when updating the controller application with a specially crafted project file exists in Modicon M580 CPU (part numbers BMEP* and BMEH*, all versions), Modicon M340 CPU (part numbers BMXP34*, all versions), Modicon MC80 (part numbers BMKC80*, all versions), Modicon Momentum Ethernet CPU (part numbers 171CBU*, all versions), PLC Simulator for EcoStruxure ^a Control Expert, including all Unity Pro versions (former name of EcoStruxure ^a Control Expert,	https://down load.schneide r- electric.com/f iles?p_Doc_Re f=SEVD- 2021-222-04	H-SCH-MODI- 180921/2079

CVSS Scoring Scale	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10
Dage 815 of 1474										

Out-of- bounds Read02-Sep-214All versions, PLC Simulator for EcoStruxure* Process Expert including all HDCS versions, Modicon Quantum CPU (part numbers 140CPU*, all versions), Modicon Premium CPU (part numbers TSXP5*, all versions).https://down loadscheider research controller / simulator when updating the controller application with a specially crafted project file exists in Modicon MS80 CPU (part numbers BMEP* and BMEH*, all versions), Modicon MS80 CPU (part numbers BMK294*, all versions), Modicon MS40 CPU (part numbers BMK296*, all versions), Modicon MS40 CPU (part numbers BMK296*, all versions), Modicon MS40 CPU (part numbers BMK206*, all versions), Modicon MS40 CPU (part numbers BMK206*, all versions), PLC Simulator for EcoStruxure* Control Expert, including all IDtty Pro versions (former name of EcoStruxure* Process Expert including all HDCS versions (former name of EcoStruxure* Process Expert all versions), Modiconhttps://down load.schneide r- electric.com/f iles7_Doc_Re f=SEVD- 2021-222-04	Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Out-of- bounds Read02-Sep-214A CWE-125: Out-of-bounds Read vulnerability that could cause a Denial of Service on the Modicon PLC controller / simulator when updating the controller application with a specially crafted project file exists in Modicon MS80 CPU (part numbers BMEP* and BMEH*, all versions), Modicon M340 CPU (part numbers BMXP34*, all versions), Modicon MC80 (part numbers BMKC80*, all versions), Modicon (part numbers 171CBU*, all versions), PLC Simulator for EcoStruxureª Control Expert, including all Unity Pro versions (former name of EcoStruxureª Process Expert, including all HDCS versions (former name of EcoStruxureª Process Expert,H-SCH-MODI- last l				for EcoStruxure ^ª Process Expert including all HDCS versions (former name of EcoStruxure ^ª Process Expert, all versions), Modicon Quantum CPU (part numbers 140CPU*, all versions), Modicon Premium CPU (part numbers TSXP5*, all		
Out-of- bounds Read02-Sep-214Read versions (muture to the control to the control the control the control the control to the con				CVE ID : CVE-2021-22789		
	bounds	02-Sep-21	4	Read vulnerability that could cause a Denial of Service on the Modicon PLC controller / simulator when updating the controller application with a specially crafted project file exists in Modicon M580 CPU (part numbers BMEP* and BMEH*, all versions), Modicon M340 CPU (part numbers BMXP34*, all versions), Modicon MC80 (part numbers BMKC80*, all versions), Modicon Momentum Ethernet CPU (part numbers 171CBU*, all versions), PLC Simulator for EcoStruxure ^a Control Expert, including all Unity Pro versions (former name of EcoStruxure ^a Process Expert including all HDCS versions (former name of EcoStruxure ^a Process Expert,	load.schneide r- electric.com/f iles?p_Doc_Re f=SEVD-	

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Quantum CPU (part numbers 140CPU*, all versions), Modicon Premium CPU (part numbers TSXP5*, all versions). CVE ID : CVE-2021-22790		
Out-of- bounds Write	02-Sep-21	4	A CWE-787: Out-of-bounds Write vulnerability that could cause a Denial of Service on the Modicon PLC controller / simulator when updating the controller application with a specially crafted project file exists in Modicon M580 CPU (part numbers BMEP* and BMEH*, all versions), Modicon M340 CPU (part numbers BMXP34*, all versions), Modicon MC80 (part numbers BMKC80*, all versions), Modicon Momentum Ethernet CPU (part numbers 171CBU*, all versions), PLC Simulator for EcoStruxure ^a Control Expert, including all Unity Pro versions (former name of EcoStruxure ^a Control Expert, all versions), PLC Simulator for EcoStruxure ^a Process Expert including all HDCS versions (former name of EcoStruxure ^a Process Expert, all versions), Modicon Quantum CPU (part numbers 140CPU*, all versions), Modicon Premium CPU (part numbers TSXP5*, all versions).	https://down load.schneide r- electric.com/f iles?p_Doc_Re f=SEVD- 2021-222-04	H-SCH-MODI- 180921/2081

Γ	CVSS Scoring Scale	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10
_	Page 817 of 1474										

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2021-22791		
NULL Pointer Dereference	02-Sep-21	5	A CWE-476: NULL Pointer Dereference vulnerability that could cause a Denial of Service on the Modicon PLC controller / simulator when updating the controller application with a specially crafted project file exists in Modicon M580 CPU (part numbers BMEP* and BMEH*, all versions), Modicon M340 CPU (part numbers BMXP34*, all versions), Modicon MC80 (part numbers BMKC80*, all versions), Modicon Momentum Ethernet CPU (part numbers 171CBU*, all versions), PLC Simulator for EcoStruxure ^a Control Expert, including all Unity Pro versions (former name of EcoStruxure ^a Control Expert, all versions), PLC Simulator for EcoStruxure ^a Process Expert including all HDCS versions (former name of EcoStruxure ^a Process Expert, all versions), Modicon Quantum CPU (part numbers 140CPU*, all versions), Modicon Premium CPU (part numbers TSXP5*, all versions). CVE ID : CVE-2021-22792	https://down load.schneide r- electric.com/f iles?p_Doc_Re f=SEVD- 2021-222-04	H-SCH-MODI- 180921/2082
modicon_qua	antum_140cp	u6515	0c		
Improper Restriction	02-Sep-21	4	A CWE-119: Improper Restriction of Operations	https://down load.schneide	H-SCH-MODI- 180921/2083
CVSS Scoring Sc	ale 0-1	1-2	2-3 3-4 4-5 5-6 Page 818 of 1474	6-7 7-8	8-9 <mark>9-10</mark>

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID		
of Operations within the Bounds of a Memory Buffer			<pre>within the Bounds of a Memory Buffer vulnerability that could cause a Denial of Service on the Modicon PLC controller / simulator when updating the controller application with a specially crafted project file exists in Modicon M580 CPU (part numbers BMEP* and BMEH*, all versions), Modicon M340 CPU (part numbers BMXP34*, all versions), Modicon MC80 (part numbers BMKC80*, all versions), Modicon Momentum Ethernet CPU (part numbers 171CBU*, all versions), PLC Simulator for EcoStruxure^a Control Expert, including all Unity Pro versions (former name of EcoStruxure^a Control Expert, all versions), PLC Simulator for EcoStruxure^a Process Expert including all HDCS versions (former name of EcoStruxure^a Process Expert, all versions), Modicon Quantum CPU (part numbers 140CPU*, all versions), Modicon Premium CPU (part numbers TSXP5*, all versions). CVE ID : CVE-2021-22789</pre>	r- electric.com/f iles?p_Doc_Re f=SEVD- 2021-222-04			
Out-of- bounds Read	02-Sep-21	4	A CWE-125: Out-of-bounds Read vulnerability that could cause a Denial of Service on the Modicon PLC controller / simulator when updating the	https://down load.schneide r- electric.com/f iles?p_Doc_Re	H-SCH-MODI- 180921/2084		
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
			controller application with a specially crafted project file exists in Modicon M580 CPU (part numbers BMEP* and BMEH*, all versions), Modicon M340 CPU (part numbers BMXP34*, all versions), Modicon MC80 (part numbers BMKC80*, all versions), Modicon Momentum Ethernet CPU (part numbers 171CBU*, all versions), PLC Simulator for EcoStruxure ^a Control Expert, including all Unity Pro versions (former name of EcoStruxure ^a Control Expert, all versions), PLC Simulator for EcoStruxure ^a Process Expert including all HDCS versions (former name of EcoStruxure ^a Process Expert, all versions), Modicon Quantum CPU (part numbers 140CPU*, all versions), Modicon Premium CPU (part numbers TSXP5*, all versions).	f=SEVD- 2021-222-04	
Out-of- bounds Write	02-Sep-21	4	A CWE-787: Out-of-bounds Write vulnerability that could cause a Denial of Service on the Modicon PLC controller / simulator when updating the controller application with a specially crafted project file exists in Modicon M580 CPU (part numbers BMEP* and BMEH*, all versions), Modicon M340 CPU (part	https://down load.schneide r- electric.com/f iles?p_Doc_Re f=SEVD- 2021-222-04	H-SCH-MODI- 180921/2085

NULL 02-Sep-21 5 A CWE-476: NULL Pointer Dereference vulnerability that could cause a Denial of Service on the Modicon M280 (part numbers SBMCR30*, all versions), Modicon MC80 (part numbers 171CBU*, all versions), PLC Simulator for EcoStruxure* Control Expert, including all Unity Proversions (former name of EcoStruxure* Control Expert, all versions), PLC Simulator for EcoStruxure* Torcess Expert including all HDCS versions (former name of EcoStruxure* Process Expert, all versions), Modicon Quantum CPU (part numbers 140CPU*, all versions), Modicon Quantum CPU (part numbers 140CPU*, all versions), Modicon Quantum CPU (part numbers 1240CPU*, all versions), Modicon Quantum CPU (part numbers TSXP5*, all versions). H-SCH-MODI-10021/2086 NULL 02-Sep-21 5 A CWE-476: NULL Pointer Dereference vulnerability that could cause a Denial of Service on the Modicon PLC controller / simulator when updating the controller application with a specially crafted project file exists in Modicon M580 CPU (part numbers BMEP* and BMEH*, all versions), Modicon M340 CPU (part numbers BMEP* and BMEH*, all versions), Modicon M240 CPU (part numbers BMEP* and BMEH*, all versions), Modicon M240 CPU (part numbers BMEP* and BMEH*, all versions), Modicon M240 CPU (part numbers BMEP* and BMEH*, all versions), Modicon M240 CPU (part numbers BMEP* and BMEH*, all versions), Modicon M240 CPU (part numbers BMEP* and BMEH*, all versions), Modicon M240 CPU (part numbers BMEP* and BMEH*, all versions), Modicon M240 CPU (part numbers BMEP* and BMEH*, all versions), Modicon M240 CPU (part numbers BMEP* and BMEH*, all versions), Modicon M240 CPU (part numbers BMEP* and BMEH*, all versions), Modicon M240 CPU (part numbers BMEP* and BMEH*, all versions), Modicon M240 CPU (part numbers BMEP* and BMEH*, all versions)	Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
NULL Pointer DereferenceDereference vulnerability that could cause a Denial of Service on the Modicon PLC controller / simulator when updating the controllerhttps://down load.schneide electric.com/f iles?p_Doc_Re f=SEVD- 2021-222-04H-SCH-MODI- 180921/2086NULL Pointer Dereference02-Sep-215Modicon M580 CPU (part numbers BMEP* and BMEH*, all versions), Modicon M340 (F=SEVD- 2021-222-04H-SCH-MODI- 180921/2086				versions), Modicon MC80 (part numbers BMKC80*, all versions), Modicon Momentum Ethernet CPU (part numbers 171CBU*, all versions), PLC Simulator for EcoStruxure ^a Control Expert, including all Unity Pro versions (former name of EcoStruxure ^a Control Expert, all versions), PLC Simulator for EcoStruxure ^a Process Expert including all HDCS versions (former name of EcoStruxure ^a Process Expert, all versions), Modicon Quantum CPU (part numbers 140CPU*, all versions), Modicon Premium CPU (part numbers TSXP5*, all versions).		
versions), Modicon Momentum Ethernet CPU	Pointer	02-Sep-21	5	Dereference vulnerability that could cause a Denial of Service on the Modicon PLC controller / simulator when updating the controller application with a specially crafted project file exists in Modicon M580 CPU (part numbers BMEP* and BMEH*, all versions), Modicon M340 CPU (part numbers BMXP34*, all versions), Modicon MC80 (part numbers BMKC80*, all versions), Modicon	load.schneide r- electric.com/f iles?p_Doc_Re f=SEVD-	

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			(part numbers 171CBU*, all versions), PLC Simulator for EcoStruxure ^a Control Expert, including all Unity Pro versions (former name of EcoStruxure ^a Control Expert, all versions), PLC Simulator for EcoStruxure ^a Process Expert including all HDCS versions (former name of EcoStruxure ^a Process Expert, all versions), Modicon Quantum CPU (part numbers 140CPU*, all versions), Modicon Premium CPU (part numbers TSXP5*, all versions). CVE ID : CVE-2021-22792		
modicon_qua	antum_140cp	u6516			
Improper Restriction of Operations within the Bounds of a Memory Buffer	02-Sep-21	4	A CWE-119: Improper Restriction of Operations within the Bounds of a Memory Buffer vulnerability that could cause a Denial of Service on the Modicon PLC controller / simulator when updating the controller application with a specially crafted project file exists in Modicon M580 CPU (part numbers BMEP* and BMEH*, all versions), Modicon M340 CPU (part numbers BMXP34*, all versions), Modicon MC80 (part numbers BMKC80*, all versions), Modicon Momentum Ethernet CPU (part numbers 171CBU*, all	https://down load.schneide r- electric.com/f iles?p_Doc_Re f=SEVD- 2021-222-04	H-SCH-MODI- 180921/2087

CVSS Scoring Scale	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10
			D	aga 022 g	£1474					

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			versions), PLC Simulator for EcoStruxure ^a Control Expert, including all Unity Pro versions (former name of EcoStruxure ^a Control Expert, all versions), PLC Simulator for EcoStruxure ^a Process Expert including all HDCS versions (former name of EcoStruxure ^a Process Expert, all versions), Modicon Quantum CPU (part numbers 140CPU*, all versions), Modicon Premium CPU (part numbers TSXP5*, all versions).		
Out-of- bounds Read	02-Sep-21	4	A CWE-125: Out-of-bounds Read vulnerability that could cause a Denial of Service on the Modicon PLC controller / simulator when updating the controller application with a specially crafted project file exists in Modicon M580 CPU (part numbers BMEP* and BMEH*, all versions), Modicon M340 CPU (part numbers BMXP34*, all versions), Modicon MC80 (part numbers BMKC80*, all versions), Modicon Momentum Ethernet CPU (part numbers 171CBU*, all versions), PLC Simulator for EcoStruxure ^a Control Expert, including all Unity Pro versions (former name of EcoStruxure ^a Control Expert, all versions), PLC Simulator	https://down load.schneide r- electric.com/f iles?p_Doc_Re f=SEVD- 2021-222-04	H-SCH-MODI- 180921/2088

Out-of- bounds02-Sep-214for EcoStruxure ^a Process Expert including all HDCS versions (former name of EcoStruxure ^a Process Expert, all versions), Modicon Quantum CPU (part numbers 140/CPU*, all versions), Modicon Premium CPU (part numbers TSXP5*, all versions)Verter U: CVE ID : CVE-2021-22790A CWE-787: Out-of-bounds Write vulnerability that could cause a Denial of Service on the Modicon PLC controller / simulator when updating the controller application with a specially crafted project file exists in Modicon M580 CPU (part numbers BMEP* and BMEH*, all versions), Modicon M680 (part numbers BMK280*, all versions), Modicon M680 (part numbers 171CBU*, all versions), Modicon M680 (part numbers 171CBU*, all versions), PLC Simulator for EcoStruxure* Control Expert, all versions), PLC Simulator for EcoStruxure* Control Expert, all versions), PLC Simulator for EcoStruxure* Control Expert, all versions), PLC Simulator for EcoStruxure* Control Expert, all versions), PLC Simulator for EcoStruxure* Process Expert including all HDCS versions (former name of EcoStruxure* Process Expert including all HDCS 	Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Out-of- bounds02-Sep-214Kase a Denial of Service on the Modicon PLC controller / simulator when updating the controller application with a specially crafted project file exists in Modicon M580 CPU (part numbers BMEP* and BMEH*, all versions), Modicon M340 CPU (part numbers BMXP34*, all versions), Modicon MC800 (part numbers BMKC80*, all versions), Modicon MC80 iles?p_Doc_Re (part numbers 171CBU*, all versions), PLC Simulator for EcoStruxureª Control Expert, all versions), PLC Simulator for EcoStruxureª Process Expert including all HDCSH-SCH-MODI- 180921/2089				Expert including all HDCS versions (former name of EcoStruxure ^a Process Expert, all versions), Modicon Quantum CPU (part numbers 140CPU*, all versions), Modicon Premium CPU (part numbers TSXP5*, all versions).		
	bounds	02-Sep-21	4	Write vulnerability that couldcause a Denial of Service onthe Modicon PLC controller /simulator when updating thecontroller application with aspecially crafted project fileexists in Modicon M580 CPU(part numbers BMEP* andBMEH*, all versions),Modicon M340 CPU (partnumbers BMXP34*, allversions), Modicon MC80(part numbers BMKC80*, allversions), ModiconMomentum Ethernet CPU(part numbers 171CBU*, allversions), PLC Simulator forEcoStruxureª Control Expert,including all Unity Proversions), PLC Simulatorfor EcoStruxureª ProcessExpert including all HDCSversions (former name ofEcoStruxureª Process Expert,all versions), Modicon	load.schneide r- electric.com/f iles?p_Doc_Re f=SEVD-	

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Weakness	Publish Date	CVSS	140CPU*, all versions), Modicon Premium CPU (part numbers TSXP5*, all versions). CVE ID : CVE-2021-22791 A CWE-476: NULL Pointer Dereference vulnerability that could cause a Denial of Service on the Modicon PLC controller / simulator when updating the controller application with a specially crafted project file exists in Modicon M580 CPU (part numbers BMEP* and BMEH*, all versions), Modicon M340 CPU (part numbers BMXP34*, all versions),	Patch	NCIIPC ID
NULL Pointer Dereference	02-Sep-21	5		https://down load.schneide r- electric.com/f iles?p_Doc_Re f=SEVD- 2021-222-04	H-SCH-MODI- 180921/2090

CVSS Scoring Scale	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10
Page 825 of 1474										

Out-of- bounds Read	02-Sep-21	4	A CWE-125: Out-of-bounds Read vulnerability that could cause a Denial of Service on the Modicon PLC controller / simulator when updating the controller application with a specially crafted project file exists in Modicon M580 CPU (part numbers BMEP* and BMEH*, all versions), Modicon M340 CPU (part numbers BMXP34*, all versions), Modicon MC80 (part numbers BMKC80*, all versions), Modicon MC80 (part numbers BMKC80*, all versions), Modicon Momentum Ethernet CPU (part numbers 171CBU*, all versions), PLC Simulator for EcoStruxure ^a Control Expert, including all Unity Pro versions (former name of EcoStruxure ^a Control Expert, all versions), PLC Simulator for EcoStruxure ^a Process Expert including all HDCS versions (former name of EcoStruxure ^a Process Expert, all versions), Modicon Quantum CPU (part numbers 140CPU*, all versions), Modicon Premium CPU (part numbers TSXP5*, all versions).	https://down load.schneide r- electric.com/f iles?p_Doc_Re f=SEVD- 2021-222-04	H-SCH-MODI- 180921/2092
Out-of- bounds Write	02-Sep-21	4	A CWE-787: Out-of-bounds Write vulnerability that could cause a Denial of Service on the Modicon PLC controller / simulator when updating the controller application with a	https://down load.schneide r- electric.com/f iles?p_Doc_Re f=SEVD-	H-SCH-MODI- 180921/2093

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			specially crafted project file exists in Modicon M580 CPU (part numbers BMEP* and BMEH*, all versions), Modicon M340 CPU (part numbers BMXP34*, all versions), Modicon MC80 (part numbers BMKC80*, all versions), Modicon Momentum Ethernet CPU (part numbers 171CBU*, all versions), PLC Simulator for EcoStruxure ^a Control Expert, including all Unity Pro versions (former name of EcoStruxure ^a Control Expert, all versions), PLC Simulator for EcoStruxure ^a Process Expert including all HDCS versions (former name of EcoStruxure ^a Process Expert, all versions), Modicon Quantum CPU (part numbers 140CPU*, all versions), Modicon Premium CPU (part numbers TSXP5*, all versions).	2021-222-04	
NULL Pointer Dereference	02-Sep-21	5	A CWE-476: NULL Pointer Dereference vulnerability that could cause a Denial of Service on the Modicon PLC controller / simulator when updating the controller application with a specially crafted project file exists in Modicon M580 CPU (part numbers BMEP* and BMEH*, all versions), Modicon M340 CPU (part numbers	https://down load.schneide r- electric.com/f iles?p_Doc_Re f=SEVD- 2021-222-04	H-SCH-MODI- 180921/2094
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 & CVE ID	Patch	NCIIPC ID
			BMXP34*, all versions), Modicon MC80 (part numbers BMKC80*, all versions), Modicon Momentum Ethernet CPU (part numbers 171CBU*, all versions), PLC Simulator for EcoStruxure ^a Control Expert, including all Unity Pro versions (former name of EcoStruxure ^a Control Expert, all versions), PLC Simulator for EcoStruxure ^a Process Expert including all HDCS versions (former name of EcoStruxure ^a Process Expert, all versions), Modicon Quantum CPU (part numbers 140CPU*, all versions), Modicon Premium CPU (part numbers TSXP5*, all versions). CVE ID : CVE-2021-22792		
plc_simulato	r_for_ecostru	xure_c	ontrol_expert	Γ	
Improper Restriction of Operations within the Bounds of a Memory Buffer	02-Sep-21	4	A CWE-119: Improper Restriction of Operations within the Bounds of a Memory Buffer vulnerability that could cause a Denial of Service on the Modicon PLC controller / simulator when updating the controller application with a specially crafted project file exists in Modicon M580 CPU (part numbers BMEP* and BMEH*, all versions), Modicon M340 CPU (part numbers BMXP34*, all versions),	https://down load.schneide r- electric.com/f iles?p_Doc_Re f=SEVD- 2021-222-04	H-SCH-PLC 180921/2095

CVSS Scoring Scale	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10
Page 829 of 1474										

			Modicon MC80 (part numbers BMKC80*, all versions), Modicon Momentum Ethernet CPU		
			(part numbers 171CBU*, all versions), PLC Simulator for EcoStruxure ^a Control Expert, including all Unity Pro versions (former name of EcoStruxure ^a Control Expert, all versions), PLC Simulator for EcoStruxure ^a Process Expert including all HDCS versions (former name of EcoStruxure ^a Process Expert, all versions), Modicon Quantum CPU (part numbers 140CPU*, all versions), Modicon Premium CPU (part numbers TSXP5*, all versions). CVE ID : CVE-2021-22789		
Out-of- bounds 07 Read)2-Sep-21	4	A CWE-125: Out-of-bounds Read vulnerability that could cause a Denial of Service on the Modicon PLC controller / simulator when updating the controller application with a specially crafted project file exists in Modicon M580 CPU (part numbers BMEP* and BMEH*, all versions), Modicon M340 CPU (part numbers BMXP34*, all versions), Modicon MC80 (part numbers BMKC80*, all versions), Modicon Momentum Ethernet CPU (part numbers 171CBU*, all versions), PLC Simulator for	https://down load.schneide r- electric.com/f iles?p_Doc_Re f=SEVD- 2021-222-04	H-SCH-PLC 180921/2096

Page 830 of 1474

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			EcoStruxure ^a Control Expert, including all Unity Pro versions (former name of EcoStruxure ^a Control Expert, all versions), PLC Simulator for EcoStruxure ^a Process Expert including all HDCS versions (former name of EcoStruxure ^a Process Expert, all versions), Modicon Quantum CPU (part numbers 140CPU*, all versions), Modicon Premium CPU (part numbers TSXP5*, all versions). CVE ID : CVE-2021-22790		
Out-of- bounds Write	02-Sep-21	4	A CWE-787: Out-of-bounds Write vulnerability that could cause a Denial of Service on the Modicon PLC controller / simulator when updating the controller application with a specially crafted project file exists in Modicon M580 CPU (part numbers BMEP* and BMEH*, all versions), Modicon M340 CPU (part numbers BMXP34*, all versions), Modicon MC80 (part numbers BMKC80*, all versions), Modicon Momentum Ethernet CPU (part numbers 171CBU*, all versions), PLC Simulator for EcoStruxure ^a Control Expert, including all Unity Pro versions (former name of EcoStruxure ^a Control Expert, all versions), PLC Simulator	https://down load.schneide r- electric.com/f iles?p_Doc_Re f=SEVD- 2021-222-04	H-SCH-PLC 180921/2097

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Expert including all HDCS versions (former name of EcoStruxure ^a Process Expert, all versions), Modicon Quantum CPU (part numbers 140CPU*, all versions), Modicon Premium CPU (part numbers TSXP5*, all versions). CVE ID : CVE-2021-22791		
NULL Pointer Dereference	02-Sep-21	5	A CWE-476: NULL Pointer Dereference vulnerability that could cause a Denial of Service on the Modicon PLC controller / simulator when updating the controller application with a specially crafted project file exists in Modicon M580 CPU (part numbers BMEP* and BMEH*, all versions), Modicon M340 CPU (part numbers BMXP34*, all versions), Modicon MC80 (part numbers BMKC80*, all versions), Modicon Momentum Ethernet CPU (part numbers 171CBU*, all versions), PLC Simulator for EcoStruxure ^a Control Expert, including all Unity Pro versions (former name of EcoStruxure ^a Control Expert, all versions), PLC Simulator for EcoStruxure ^a Process Expert including all HDCS versions (former name of EcoStruxure ^a Process Expert, all versions), Modicon Quantum CPU (part numbers	https://down load.schneide r- electric.com/f iles?p_Doc_Re f=SEVD- 2021-222-04	H-SCH-PLC 180921/2098
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 & CVE ID	Patch	NCIIPC ID
plc_simulato	r_for_ecostru	xure_p	140CPU*, all versions), Modicon Premium CPU (part numbers TSXP5*, all versions). CVE ID : CVE-2021-22792 rocess_expert		
Improper Restriction of Operations within the Bounds of a Memory Buffer	02-Sep-21	4	A CWE-119: Improper Restriction of Operations within the Bounds of a Memory Buffer vulnerability that could cause a Denial of Service on the Modicon PLC controller / simulator when updating the controller application with a specially crafted project file exists in Modicon M580 CPU (part numbers BMEP* and BMEH*, all versions), Modicon M340 CPU (part numbers BMXP34*, all versions), Modicon MC80 (part numbers BMKC80*, all versions), Modicon Momentum Ethernet CPU (part numbers 171CBU*, all versions), PLC Simulator for EcoStruxure ^a Control Expert, including all Unity Pro versions (former name of EcoStruxure ^a Control Expert, all versions), PLC Simulator for EcoStruxure ^a Process Expert including all HDCS versions (former name of EcoStruxure ^a Process Expert, all versions), Modicon Quantum CPU (part numbers 140CPU*, all versions),	https://down load.schneide r- electric.com/f iles?p_Doc_Re f=SEVD- 2021-222-04	H-SCH-PLC 180921/2099

CVSS Scoring Scale	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10
Dage 922 of 1474										

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Weakness Out-of- bounds Read	Publish Date	CVSS	Description & CVE IDModicon Premium CPU (partnumbers TSXP5*, allversions).CVE ID : CVE-2021-22789A CWE-125: Out-of-boundsRead vulnerability that couldcause a Denial of Service onthe Modicon PLC controller /simulator when updating thecontroller application with aspecially crafted project fileexists in Modicon M580 CPU(part numbers BMEP* andBMEH*, all versions),Modicon M340 CPU (partnumbers BMXP34*, allversions), Modicon MC80(part numbers BMKC80*, allversions), ModiconMomentum Ethernet CPU(part numbers 171CBU*, allversions), PLC Simulator forEcoStruxureª Control Expert,all versions), PLC Simulatorfor EcoStruxureª Control Expert,all versions), PLC Simulatorfor EcoStruxureª ProcessExpert including all HDCSversions (former name ofEcoStruxureª Process Expert,all versions), ModiconQuantum CPU (part numbers140CPU*, all versions),Modicon Premium CPU (partnumbers TSXP5*, all	Patch https://down load.schneide r- electric.com/f iles?p_Doc_Re f=SEVD- 2021-222-04	NCIIPC ID
			versions). CVE ID : CVE-2021-22790		
Out-of-	02-Sep-21	4	A CWE-787: Out-of-bounds	https://down	H-SCH-PLC

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
bounds Write			Write vulnerability that couldcause a Denial of Service onthe Modicon PLC controller /simulator when updating thecontroller application with aspecially crafted project fileexists in Modicon M580 CPU(part numbers BMEP* andBMEH*, all versions),Modicon M340 CPU (partnumbers BMXP34*, allversions), Modicon MC80(part numbers BMKC80*, allversions), Modicon MC80(part numbers BMKC80*, allversions), ModiconMomentum Ethernet CPU(part numbers 171CBU*, allversions), PLC Simulator forEcoStruxureª Control Expert,including all Unity Proversions (former name ofEcoStruxureª Control Expert,all versions), PLC Simulatorfor EcoStruxureª ProcessExpert including all HDCSversions (former name ofEcoStruxureª Process Expert,all versions), ModiconQuantum CPU (part numbers140CPU*, all versions),Modicon Premium CPU (partnumbers TSXP5*, allversions).CVE ID : CVE-2021-22791	load.schneide r- electric.com/f iles?p_Doc_Re f=SEVD- 2021-222-04	180921/2101
NULL Pointer Dereference CVSS Scoring Sc	02-Sep-21 ale 0-1	5	A CWE-476: NULL Pointer Dereference vulnerability that could cause a Denial of Service on the Modicon PLC controller / simulator when updating the controller application with a specially 2-3 3-4 4-5 5-6	https://down load.schneide r- electric.com/f iles?p_Doc_Re f=SEVD-	H-SCH-PLC 180921/2102 8-9 9-10

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			crafted project file exists in Modicon M580 CPU (part numbers BMEP* and BMEH*, all versions), Modicon M340 CPU (part numbers BMXP34*, all versions), Modicon MC80 (part numbers BMKC80*, all versions), Modicon Momentum Ethernet CPU (part numbers 171CBU*, all versions), PLC Simulator for EcoStruxure ^a Control Expert, including all Unity Pro versions (former name of EcoStruxure ^a Control Expert, all versions), PLC Simulator for EcoStruxure ^a Process Expert including all HDCS versions (former name of EcoStruxure ^a Process Expert, all versions), Modicon Quantum CPU (part numbers 140CPU*, all versions), Modicon Premium CPU (part numbers TSXP5*, all versions). CVE ID : CVE-2021-22792	2021-222-04	
silabs					
wt32i-a					
N/A	07-Sep-21	3.3	The Bluetooth Classic implementation in Silicon Labs iWRAP 6.3.0 and earlier does not properly handle the reception of an oversized LMP packet greater than 17 bytes, allowing attackers in radio range to trigger a crash in WT32i via a crafted LMP	https://www. silabs.com/wi reless/blueto oth/bluegiga- classic- legacy- modules/devi ce.wt32i-a	H-SIL-WT32- 180921/2103
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 & CVE ID	Patch	NCIIPC ID
			packet.		
			CVE ID : CVE-2021-31609		
ti					
cc256xcqfn-e	em				
N/A	07-Sep-21	3.3	The Bluetooth Classic implementation on the Texas Instruments CC256XCQFN- EM does not properly handle the reception of continuous LMP_AU_Rand packets, allowing attackers in radio range to trigger a denial of service (deadlock) of the device by flooding it with LMP_AU_Rand packets after the paging procedure. CVE ID : CVE-2021-34149	https://www. ti.com/produ ct/CC2564C, https://www. ti.com/tool/C C256XC-BT- SP#primary- sw	H-TI-CC25- 180921/2104
zh-jieli					
ac6901					
N/A	07-Sep-21	3.3	The Bluetooth Classic implementation on Zhuhai Jieli AC690X and AC692X devices does not properly handle an out-of-order LMP Setup procedure that is followed by a malformed LMP packet, allowing attackers in radio range to deadlock a device via a crafted LMP packet. The user needs to manually reboot the device to restore communication. CVE ID : CVE-2021-31611	http://www. zh- jieli.com/pro duct/68- cn.html	H-ZHAC69- 180921/2105
N/A	07-Sep-21	6.1	The Bluetooth Classic implementation on Zhuhai Jieli AC690X devices does not	http://www. zh- jieli.com/pro	H-ZHAC69- 180921/2106
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 & CVE ID	Patch	NCIIPC ID
			properly handle the reception of an oversized LMP packet greater than 17 bytes during the LMP auto rate procedure, allowing attackers in radio range to trigger a deadlock via a crafted LMP packet. CVE ID : CVE-2021-31612	duct/68- cn.html	
N/A	07-Sep-21	3.3	The Bluetooth Classic implementation on Zhuhai Jieli AC690X and AC692X devices does not properly handle the reception of a truncated LMP packet during the LMP auto rate procedure, allowing attackers in radio range to immediately crash (and restart) a device via a crafted LMP packet. CVE ID : CVE-2021-31613	http://www. zh- jieli.com/pro duct/68- cn.html	H-ZHAC69- 180921/2107
ac6902					
N/A	07-Sep-21	6.1	The Bluetooth Classic implementation on Zhuhai Jieli AC690X devices does not properly handle the reception of an oversized LMP packet greater than 17 bytes during the LMP auto rate procedure, allowing attackers in radio range to trigger a deadlock via a crafted LMP packet. CVE ID : CVE-2021-31612	http://www. zh- jieli.com/pro duct/68- cn.html	H-ZHAC69- 180921/2108
ac6903					
N/A	07-Sep-21	6.1	The Bluetooth Classic implementation on Zhuhai Jieli AC690X devices does not	http://www. zh- jieli.com/pro	H-ZHAC69- 180921/2109
CVSS Scoring So	cale 0-1	1-2	2-3 3-4 4-5 5-6 Page 838 of 1474	6-7 7-8	8-9 9-10

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			properly handle the reception of an oversized LMP packet greater than 17 bytes during the LMP auto rate procedure, allowing attackers in radio range to trigger a deadlock via a crafted LMP packet. CVE ID : CVE-2021-31612	duct/68- cn.html	
ac6904				1	
N/A	07-Sep-21	6.1	The Bluetooth Classic implementation on Zhuhai Jieli AC690X devices does not properly handle the reception of an oversized LMP packet greater than 17 bytes during the LMP auto rate procedure, allowing attackers in radio range to trigger a deadlock via a crafted LMP packet. CVE ID : CVE-2021-31612	http://www. zh- jieli.com/pro duct/68- cn.html	H-ZHAC69- 180921/2110
ac6905					
N/A	07-Sep-21	6.1	The Bluetooth Classic implementation on Zhuhai Jieli AC690X devices does not properly handle the reception of an oversized LMP packet greater than 17 bytes during the LMP auto rate procedure, allowing attackers in radio range to trigger a deadlock via a crafted LMP packet. CVE ID : CVE-2021-31612	http://www. zh- jieli.com/pro duct/68- cn.html	H-ZHAC69- 180921/2111
ac6907					
N/A	07-Sep-21	6.1	The Bluetooth Classic	http://www.	H-ZHAC69-
CVSS Scoring Sc	cale 0-1	1-2	2-3 3-4 4-5 5-6 Page 839 of 1474	6-7 7-8	8-9 9-10

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			implementation on Zhuhai Jieli AC690X devices does not properly handle the reception of an oversized LMP packet greater than 17 bytes during the LMP auto rate procedure, allowing attackers in radio range to trigger a deadlock via a crafted LMP packet. CVE ID : CVE-2021-31612	zh- jieli.com/pro duct/68- cn.html	180921/2112
ac6908					
N/A	07-Sep-21	6.1	The Bluetooth Classic implementation on Zhuhai Jieli AC690X devices does not properly handle the reception of an oversized LMP packet greater than 17 bytes during the LMP auto rate procedure, allowing attackers in radio range to trigger a deadlock via a crafted LMP packet. CVE ID : CVE-2021-31612	http://www. zh- jieli.com/pro duct/68- cn.html	H-ZHAC69- 180921/2113
ac690n					
N/A	07-Sep-21	6.1	The Bluetooth Classic implementation on Zhuhai Jieli AC690X devices does not properly handle the reception of an oversized LMP packet greater than 17 bytes during the LMP auto rate procedure, allowing attackers in radio range to trigger a deadlock via a crafted LMP packet. CVE ID : CVE-2021-31612	http://www. zh- jieli.com/pro duct/68- cn.html	H-ZHAC69- 180921/2114

CVSS Scoring Scale	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10
Page 840 of 1474										

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
ac6921					
N/A	07-Sep-21	3.3	The Bluetooth Classic implementation on Zhuhai Jieli AC690X and AC692X devices does not properly handle an out-of-order LMP Setup procedure that is followed by a malformed LMP packet, allowing attackers in radio range to deadlock a device via a crafted LMP packet. The user needs to manually reboot the device to restore communication. CVE ID : CVE-2021-31611	http://www. zh- jieli.com/pro duct/68- cn.html	H-ZHAC69- 180921/2115
N/A	07-Sep-21	3.3	The Bluetooth Classic implementation on Zhuhai Jieli AC690X and AC692X devices does not properly handle the reception of a truncated LMP packet during the LMP auto rate procedure, allowing attackers in radio range to immediately crash (and restart) a device via a crafted LMP packet. CVE ID : CVE-2021-31613	http://www. zh- jieli.com/pro duct/68- cn.html	H-ZHAC69- 180921/2116
ac6925					
N/A	07-Sep-21	3.3	The Bluetooth Classic implementation on Zhuhai Jieli AC690X and AC692X devices does not properly handle an out-of-order LMP Setup procedure that is followed by a malformed LMP packet, allowing attackers in radio range to	http://www. zh- jieli.com/pro duct/68- cn.html	H-ZHAC69- 180921/2117

CVSS Scoring Scale	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10
			D	200 9/1 0	f 1/7/					

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			deadlock a device via a crafted LMP packet. The user needs to manually reboot the device to restore communication. CVE ID : CVE-2021-31611		
N/A	07-Sep-21	3.3	The Bluetooth Classic implementation on Zhuhai Jieli AC690X and AC692X devices does not properly handle the reception of a truncated LMP packet during the LMP auto rate procedure, allowing attackers in radio range to immediately crash (and restart) a device via a crafted LMP packet.	http://www. zh- jieli.com/pro duct/68- cn.html	H-ZHAC69- 180921/2118
600.6			CVE ID : CVE-2021-31613		
ac6926	ſ				
N/A	07-Sep-21	3.3	The Bluetooth Classic implementation on Zhuhai Jieli AC690X and AC692X devices does not properly handle an out-of-order LMP Setup procedure that is followed by a malformed LMP packet, allowing attackers in radio range to deadlock a device via a crafted LMP packet. The user needs to manually reboot the device to restore communication. CVE ID : CVE-2021-31611	http://www. zh- jieli.com/pro duct/68- cn.html	H-ZHAC69- 180921/2119
N/A	07-Sep-21	3.3	The Bluetooth Classic implementation on Zhuhai Jieli AC690X and AC692X devices does not properly	http://www. zh- jieli.com/pro duct/68-	H-ZHAC69- 180921/2120
CVSS Scoring Sc	ale 0-1	1-2	2-3 3-4 4-5 5-6	6-7 7-8	8-9 9-10

Page 842 of 1474

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			handle the reception of a truncated LMP packet during the LMP auto rate procedure, allowing attackers in radio range to immediately crash (and restart) a device via a crafted LMP packet. CVE ID : CVE-2021-31613	cn.html	
ac6928					
N/A	07-Sep-21	3.3	The Bluetooth Classic implementation on Zhuhai Jieli AC690X and AC692X devices does not properly handle an out-of-order LMP Setup procedure that is followed by a malformed LMP packet, allowing attackers in radio range to deadlock a device via a crafted LMP packet. The user needs to manually reboot the device to restore communication. CVE ID : CVE-2021-31611	http://www. zh- jieli.com/pro duct/68- cn.html	H-ZHAC69- 180921/2121
N/A	07-Sep-21	3.3	The Bluetooth Classic implementation on Zhuhai Jieli AC690X and AC692X devices does not properly handle the reception of a truncated LMP packet during the LMP auto rate procedure, allowing attackers in radio range to immediately crash (and restart) a device via a crafted LMP packet. CVE ID : CVE-2021-31613	http://www. zh- jieli.com/pro duct/68- cn.html	H-ZHAC69- 180921/2122
ac692n				1	

CVSS Scoring Scale

0-1

1-2

5-6

6-7

7-8

8-9

9-10

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
N/A	07-Sep-21	6.1	The Bluetooth Classic implementation on Zhuhai Jieli AC690X devices does not properly handle the reception of an oversized LMP packet greater than 17 bytes during the LMP auto rate procedure, allowing attackers in radio range to trigger a deadlock via a crafted LMP packet. CVE ID : CVE-2021-31612	http://www. zh- jieli.com/pro duct/68- cn.html	H-ZHAC69- 180921/2123
ac6936					
N/A	07-Sep-21	6.1	The Bluetooth Classic implementation in the Zhuhai Jieli AC6366C_DEMO_V1.0 does not properly handle the reception of continuous unsolicited LMP responses, allowing attackers in radio range to trigger a denial of service (deadlock) of the device by flooding it with LMP_AU_Rand packets after paging procedure. User intervention is required to restart the device. CVE ID : CVE-2021-34143	N/A	H-ZHAC69- 180921/2124
N/A	07-Sep-21	3.3	The Bluetooth Classic implementation in the Zhuhai Jieli AC6366C BT SDK through 0.9.1 does not properly handle the reception of truncated LMP_SCO_Link_Request packets while no other BT connections are active, allowing attackers in radio range to prevent new BT	N/A	H-ZHAC69- 180921/2125

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			connections (disabling the AB5301A inquiry and page scan procedures) via a crafted LMP packet. The user needs to manually perform a power cycle (restart) of the device to restore BT connectivity. CVE ID : CVE-2021-34144		
ac6951				<u> </u>	I
N/A	07-Sep-21	6.1	The Bluetooth Classic implementation in the Zhuhai Jieli AC6366C_DEMO_V1.0 does not properly handle the reception of continuous unsolicited LMP responses, allowing attackers in radio range to trigger a denial of service (deadlock) of the device by flooding it with LMP_AU_Rand packets after paging procedure. User intervention is required to restart the device. CVE ID : CVE-2021-34143	N/A	H-ZHAC69- 180921/2126
N/A	07-Sep-21	3.3	The Bluetooth Classic implementation in the Zhuhai Jieli AC6366C BT SDK through 0.9.1 does not properly handle the reception of truncated LMP_SCO_Link_Request packets while no other BT connections are active, allowing attackers in radio range to prevent new BT connections (disabling the AB5301A inquiry and page scan procedures) via a	N/A	H-ZHAC69- 180921/2127
CVSS Scoring Sc	cale 0-1	1-2	2-3 3-4 4-5 5-6 Page 845 of 1474	6-7 7-8	8-9 9-10

Page 845 of 1474

Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
		crafted LMP packet. The user needs to manually perform a power cycle (restart) of the device to restore BT connectivity. CVE ID : CVE-2021-34144		
07-Sep-21	6.1	The Bluetooth Classic implementation in the Zhuhai Jieli AC6366C_DEMO_V1.0 does not properly handle the reception of continuous unsolicited LMP responses, allowing attackers in radio range to trigger a denial of service (deadlock) of the device by flooding it with LMP_AU_Rand packets after paging procedure. User intervention is required to restart the device. CVE ID : CVE-2021-34143	N/A	H-ZHAC69- 180921/2128
07-Sep-21	3.3	The Bluetooth Classic implementation in the Zhuhai Jieli AC6366C BT SDK through 0.9.1 does not properly handle the reception of truncated LMP_SCO_Link_Request packets while no other BT connections are active, allowing attackers in radio range to prevent new BT connections (disabling the AB5301A inquiry and page scan procedures) via a crafted LMP packet. The user needs to manually perform a power cycle (restart) of the	N/A	H-ZHAC69- 180921/2129
	07-Sep-21	07-Sep-21 6.1 Image: Non-Sep-21 Image: Non-Sep-21	O7-Sep-216.1The Bluetooth Classic implementation in the Zhuhai Jieli AC6366C_DEMO_V1.0 does not properly handle the reception of continuous unsolicited LMP responses, allowing attackers in radio range to trigger a denial of service (deadlock) of the device by flooding it with LMP_AU_Rand packets after paging procedure. User intervention is required to restart the device.07-Sep-215.107-Sep-216.107-Sep-215.107-Sep-215.107-Sep-215.107-Sep-215.107-Sep-215.107-Sep-215.107-Sep-215.107-Sep-215.107-Sep-215.107-Sep-215.307-Sep-21	07-Sep-216.1Crafted LMP packet. The user needs to manually perform a power cycle (restart) of the device to restore BT connectivity.V07-Sep-216.1The Bluetooth Classic implementation in the Zhuhai Jieli AC6366C_DEMO_V1.0 does not properly handle the reception of continuous unsolicited LMP responses, allowing attackers in radio range to trigger a denial of service (deadlock) of the device by flooding it with LMP_AU_Rand packets after paging procedure. User intervention is required to restart the device.N/A07-Sep-213.3The Bluetooth Classic implementation in the Zhuhai Jieli AC6366C_DEMO_V1.0 does not properly handle the reception of continuous unsolicited LMP responses, allowing attackers in radio range to trigger a denial of service (deadlock) of the device by flooding it with LMP_AU_Rand packets after paging procedure. User intervention is required to restart the device.07-Sep-213.3The Bluetooth Classic implementation in the Zhuhai Jieli AC6366C BT SDK through 0.9.1 does not properly handle the reception of truncated LMP_SCO_Link_Request packets while no other BT connections are active, allowing attackers in radio range to prevent new BT connections (disabling the AB5301A inquiry and page scan procedures) via a crafted LMP packet. The user needs to manually perform a

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			device to restore BT connectivity.		
			CVE ID : CVE-2021-34144		
ac6954					
N/A	07-Sep-21	6.1	The Bluetooth Classic implementation in the Zhuhai Jieli AC6366C_DEMO_V1.0 does not properly handle the reception of continuous unsolicited LMP responses, allowing attackers in radio range to trigger a denial of service (deadlock) of the device by flooding it with LMP_AU_Rand packets after paging procedure. User intervention is required to restart the device. CVE ID : CVE-2021-34143	N/A	H-ZHAC69- 180921/2130
N/A	07-Sep-21	3.3	The Bluetooth Classic implementation in the Zhuhai Jieli AC6366C BT SDK through 0.9.1 does not properly handle the reception of truncated LMP_SCO_Link_Request packets while no other BT connections are active, allowing attackers in radio range to prevent new BT connections (disabling the AB5301A inquiry and page scan procedures) via a crafted LMP packet. The user needs to manually perform a power cycle (restart) of the device to restore BT connectivity.	N/A	H-ZHAC69- 180921/2131

CVSS Scoring Scale	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10
			D	200 847 0	f 1/7/					

ac6955	07-Sep-21	6.1	CVE ID : CVE-2021-34144 The Bluetooth Classic implementation in the Zhuhai Jieli AC6366C_DEMO_V1.0 does not properly handle the reception of continuous unsolicited LMP responses, allowing attackers in radio range to trigger a denial of service (deadlock) of the	N/A	Н-ZHAC69-
	07-Sep-21	6.1	implementation in the Zhuhai Jieli AC6366C_DEMO_V1.0 does not properly handle the reception of continuous unsolicited LMP responses, allowing attackers in radio range to trigger a denial of	N/A	H-ZHAC69-
N/A	07-Sep-21	6.1	implementation in the Zhuhai Jieli AC6366C_DEMO_V1.0 does not properly handle the reception of continuous unsolicited LMP responses, allowing attackers in radio range to trigger a denial of	N/A	H-ZHAC69-
			device by flooding it with LMP_AU_Rand packets after paging procedure. User intervention is required to restart the device. CVE ID : CVE-2021-34143		180921/2132
N/A	07-Sep-21	3.3	The Bluetooth Classic implementation in the Zhuhai Jieli AC6366C BT SDK through 0.9.1 does not properly handle the reception of truncated LMP_SCO_Link_Request packets while no other BT connections are active, allowing attackers in radio range to prevent new BT connections (disabling the AB5301A inquiry and page scan procedures) via a crafted LMP packet. The user needs to manually perform a power cycle (restart) of the device to restore BT connectivity. CVE ID : CVE-2021-34144	N/A	H-ZHAC69- 180921/2133
ac6956					
CVSS Scoring Scal	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
N/A	07-Sep-21	6.1	The Bluetooth Classic implementation in the Zhuhai Jieli AC6366C_DEMO_V1.0 does not properly handle the reception of continuous unsolicited LMP responses, allowing attackers in radio range to trigger a denial of service (deadlock) of the device by flooding it with LMP_AU_Rand packets after paging procedure. User intervention is required to restart the device. CVE ID : CVE-2021-34143	N/A	H-ZHAC69- 180921/2134
N/A	07-Sep-21	3.3	The Bluetooth Classic implementation in the Zhuhai Jieli AC6366C BT SDK through 0.9.1 does not properly handle the reception of truncated LMP_SCO_Link_Request packets while no other BT connections are active, allowing attackers in radio range to prevent new BT connections (disabling the AB5301A inquiry and page scan procedures) via a crafted LMP packet. The user needs to manually perform a power cycle (restart) of the device to restore BT connectivity. CVE ID : CVE-2021-34144	N/A	H-ZHAC69- 180921/2135
ac6963					
N/A	07-Sep-21	6.1	The Bluetooth Classic implementation in the Zhuhai Jieli AC6366C_DEMO_V1.0	N/A	H-ZHAC69- 180921/2136
CVSS Scoring Sc	ale 0-1	1-2	2-3 3-4 4-5 5-6 Page 849 of 1474	6-7 7-8	8-9 9-10

			does not properly handle the reception of continuous unsolicited LMP responses, allowing attackers in radio range to trigger a denial of service (deadlock) of the device by flooding it with LMP_AU_Rand packets after paging procedure. User intervention is required to restart the device. CVE ID : CVE-2021-34143		
N/A	07-Sep-21	3.3	The Bluetooth Classic implementation in the Zhuhai Jieli AC6366C BT SDK through 0.9.1 does not properly handle the reception of truncated LMP_SCO_Link_Request packets while no other BT connections are active, allowing attackers in radio range to prevent new BT connections (disabling the AB5301A inquiry and page scan procedures) via a crafted LMP packet. The user needs to manually perform a power cycle (restart) of the device to restore BT connectivity. CVE ID : CVE-2021-34144	N/A	H-ZHAC69- 180921/2137
ac6965					
N/A	07-Sep-21	6.1	The Bluetooth Classic implementation in the Zhuhai Jieli AC6366C_DEMO_V1.0 does not properly handle the reception of continuous unsolicited LMP responses,	N/A	H-ZHAC69- 180921/2138

Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
		allowing attackers in radio range to trigger a denial of service (deadlock) of the device by flooding it with LMP_AU_Rand packets after paging procedure. User intervention is required to restart the device. CVE ID : CVE-2021-34143		
07-Sep-21	3.3	The Bluetooth Classic implementation in the Zhuhai Jieli AC6366C BT SDK through 0.9.1 does not properly handle the reception of truncated LMP_SCO_Link_Request packets while no other BT connections are active, allowing attackers in radio range to prevent new BT connections (disabling the AB5301A inquiry and page scan procedures) via a crafted LMP packet. The user needs to manually perform a power cycle (restart) of the device to restore BT connectivity. CVE ID : CVE-2021-34144	N/A	H-ZHAC69- 180921/2139
·				
07-Sep-21	6.1	The Bluetooth Classic implementation in the Zhuhai Jieli AC6366C_DEMO_V1.0 does not properly handle the reception of continuous unsolicited LMP responses, allowing attackers in radio range to trigger a denial of service (deadlock) of the	N/A	H-ZHAC69- 180921/2140
	07-Sep-21	07-Sep-21 3.3 07-Sep-21 6.1	07-Sep-213.3The Bluetooth Classic implementation in quiry and page scan procedures) via a crafted LMP packet. The user needs to manually perform a power cycle (restart) of the device to restore BT connectivity.07-Sep-216.1The Bluetooth Classic implementation in the Zhuhai jleli AC6366C BT SDK through 0.9.1 does not properly handle the reception of truncated LMP_SCO_Link_Request packets while no other BT connections are active, allowing attackers in radio range to prevent new BT connections (disabling the AB5301A inquiry and page scan procedures) via a crafted LMP packet. The user needs to manually perform a power cycle (restart) of the device to restore BT connectivity.07-Sep-216.1The Bluetooth Classic implementation in the Zhuhai jleli AC6366C_DEMO_V1.0 does not properly handle the reception of continuous unsolicited LMP responses, allowing attackers in radio range to trigger a denial of service (deadlock) of the	07-Sep-21A.A.Allowing attackers in radio range to trigger a denial of service (deadlock) of the device by flooding it with LMP_AU_Rand packets after paging procedure. User intervention is required to restart the device.CVE ID : CVE-2021-3414307-Sep-21The Bluetooth Classic implementation in the Zhuhai Jieli ACG366C BT SDK through 0.9.1 does not properly handle the reception of truncated

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			device by flooding it with LMP_AU_Rand packets after paging procedure. User intervention is required to restart the device. CVE ID : CVE-2021-34143		
N/A	07-Sep-21	3.3	The Bluetooth Classic implementation in the Zhuhai Jieli AC6366C BT SDK through 0.9.1 does not properly handle the reception of truncated LMP_SCO_Link_Request packets while no other BT connections are active, allowing attackers in radio range to prevent new BT connections (disabling the AB5301A inquiry and page scan procedures) via a crafted LMP packet. The user needs to manually perform a power cycle (restart) of the device to restore BT connectivity. CVE ID : CVE-2021-34144	N/A	H-ZHAC69- 180921/2141
ac6969					
N/A	A 07-Sep-21 6.1 implementa Jieli AC636 does not provide reception of unsolicited allowing attriange to trip service (dea device by fl LMP_AU_Ra		The Bluetooth Classic implementation in the Zhuhai Jieli AC6366C_DEMO_V1.0 does not properly handle the reception of continuous unsolicited LMP responses, allowing attackers in radio range to trigger a denial of service (deadlock) of the device by flooding it with LMP_AU_Rand packets after paging procedure. User	N/A	H-ZHAC69- 180921/2142
CVSS Scoring Sc	cale 0-1	1-2	2-3 3-4 4-5 5-6	6-7 7-8	8-9 9-10

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			intervention is required to restart the device. CVE ID : CVE-2021-34143		
N/A ac6973	07-Sep-21	3.3	The Bluetooth Classic implementation in the Zhuhai Jieli AC6366C BT SDK through 0.9.1 does not properly handle the reception of truncated LMP_SCO_Link_Request packets while no other BT connections are active, allowing attackers in radio range to prevent new BT connections (disabling the AB5301A inquiry and page scan procedures) via a crafted LMP packet. The user needs to manually perform a power cycle (restart) of the device to restore BT connectivity. CVE ID : CVE-2021-34144	N/A	H-ZHAC69- 180921/2143
ac6973	-			1	
N/A	07-Sep-21	6.1	The Bluetooth Classic implementation in the Zhuhai Jieli AC6366C_DEMO_V1.0 does not properly handle the reception of continuous unsolicited LMP responses, allowing attackers in radio range to trigger a denial of service (deadlock) of the device by flooding it with LMP_AU_Rand packets after paging procedure. User intervention is required to restart the device.	N/A	H-ZHAC69- 180921/2144

CVSS Scoring Scale	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10
Dago 952 of 1474										

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2021-34143		
N/A	07-Sep-21	3.3	The Bluetooth Classic implementation in the Zhuha Jieli AC6366C BT SDK through 0.9.1 does not properly handle the reception of truncated LMP_SCO_Link_Request packets while no other BT connections are active, allowing attackers in radio range to prevent new BT connections (disabling the AB5301A inquiry and page scan procedures) via a crafted LMP packet. The user needs to manually perform a power cycle (restart) of the device to restore BT connectivity. CVE ID : CVE-2021-34144	N/A	H-ZHAC69- 180921/2145
ac6976	F			-	
N/A	07-Sep-21	6.1	The Bluetooth Classic implementation in the Zhuha Jieli AC6366C_DEMO_V1.0 does not properly handle the reception of continuous unsolicited LMP responses, allowing attackers in radio range to trigger a denial of service (deadlock) of the device by flooding it with LMP_AU_Rand packets after paging procedure. User intervention is required to restart the device. CVE ID : CVE-2021-34143	N/A	H-ZHAC69- 180921/2146
N/A	07-Sep-21	3.3	The Bluetooth Classic	N/A	H-ZHAC69-
CVSS Scoring Sc	ale 0-1	1-2	2-3 3-4 4-5 5-6	6-7 7-8	8-9 9-10

N/A07-Sep-216.1The Bluetooth Classic implementation in the Zhuhai Jeli AC6366 GT SDK through 0.9.1 does not properly handle the reception of truncated LMP_SCO_Link, Request packets while no other BT connections are active, allowing attackers in radio range to preven new BT connections (disabling the AB5301A inquiry and page scan procedures) via a crafted LMP packet. The user needs to manually perform a power cycle (restart) of the device to restore BT connectivity. CVE ID : CVE-2021-34144180921/2147ac6983The Bluetooth Classic implementation in the Zhuhai Jeli AC6366C_DEMO_V1.0N/AH-ZH-AC69- 180921/2148N/A07-Sep-216.1The Bluetooth Classic implementation in the Zhuhai Jeli AC6366C_DEMO_V1.0N/AH-ZH-AC69- 180921/2148N/A07-Sep-215.1The Bluetooth Classic implementation in the Zhuhai Jeli AC6366C_DEMO_V1.0N/AH-ZH-AC69- 180921/2148N/A07-Sep-213.3The Bluetooth Classic implementation in the Zhuhai Jeli AC6366C_DEMO_V1.0N/AH-ZH-AC69- 180921/2148N/A07-Sep-213.3The Bluetooth Classic implementation in the Zhuhai Jeli AC6366C BT SDKN/AH-ZH-AC69- 180921/2148	Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
N/A07-Sep-21A.IThe Bluetooth Classic implementation in the Zhuhai Jieli AC6366C_DEMO_V1.0 does not properly handle the reception of continuous unsolicited LMP responses, allowing attackers in radio range to trigger a denial of service (deadlock) of the device by flooding it with LMP_AU_Rand packets after paging procedure. User intervention is required to restart the device.N/AH-ZHAC69- 180921/2148N/A07-Sep-213.3The Bluetooth Classic implementation in the Zhuhai Jieli AC6366C BT SDK throug 0.9.1 does notN/AH-ZHAC69- 180921/2148				Jieli AC6366C BT SDK through 0.9.1 does not properly handle the reception of truncated LMP_SCO_Link_Request packets while no other BT connections are active, allowing attackers in radio range to prevent new BT connections (disabling the AB5301A inquiry and page scan procedures) via a crafted LMP packet. The user needs to manually perform a power cycle (restart) of the device to restore BT connectivity.		180921/2147
N/A07-Sep-216.1implementation in the Zhuhai Jieli AC6366C_DEMO_V1.0 does not properly handle the reception of continuous unsolicited LMP responses, allowing attackers in radio range to trigger a denial of service (deadlock) of the device by flooding it with LMP_AU_Rand packets after paging procedure. User intervention is required to restart the device.N/AH-ZHAC69- 180921/2148N/A07-Sep-213.3The Bluetooth Classic implementation in the Zhuhai Jieli AC6366C BT SDK through 0.9.1 does notN/AH-ZHAC69- 180921/2149	ac6983					
N/A 07-Sep-21 3.3 implementation in the Zhuhai Jieli AC6366C BT SDK through 0.9.1 does not H-ZHAC69-180921/2149	N/A	07-Sep-21	6.1	implementation in the Zhuhai Jieli AC6366C_DEMO_V1.0 does not properly handle the reception of continuous unsolicited LMP responses, allowing attackers in radio range to trigger a denial of service (deadlock) of the device by flooding it with LMP_AU_Rand packets after paging procedure. User intervention is required to restart the device.	N/A	
				implementation in the Zhuhai Jieli AC6366C BT SDK through 0.9.1 does not		180921/2149

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			properly handle the reception of truncated LMP_SCO_Link_Request packets while no other BT connections are active, allowing attackers in radio range to prevent new BT connections (disabling the AB5301A inquiry and page scan procedures) via a crafted LMP packet. The user needs to manually perform a power cycle (restart) of the device to restore BT connectivity.		
			CVE ID : CVE-2021-34144		
ac6986	1				
N/A	07-Sep-21	6.1	The Bluetooth Classic implementation in the Zhuhai Jieli AC6366C_DEMO_V1.0 does not properly handle the reception of continuous unsolicited LMP responses, allowing attackers in radio range to trigger a denial of service (deadlock) of the device by flooding it with LMP_AU_Rand packets after paging procedure. User intervention is required to restart the device. CVE ID : CVE-2021-34143	N/A	H-ZHAC69- 180921/2150
N/A	07-Sep-21	3.3	The Bluetooth Classic implementation in the Zhuhai Jieli AC6366C BT SDK through 0.9.1 does not properly handle the reception of truncated LMP_SCO_Link_Request	N/A	H-ZHAC69- 180921/2151

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID				
			CVE ID : CVE-2021-31612	E-2021-31612					
ac6999				I	I				
N/A	07-Sep-21	6.1	The Bluetooth Classic implementation on Zhuhai Jieli AC690X devices does not properly handle the reception of an oversized LMP packet greater than 17 bytes during the LMP auto rate procedure, allowing attackers in radio range to trigger a deadlock via a crafted LMP packet.	http://www. zh- jieli.com/pro duct/68- cn.html	H-ZHAC69- 180921/2154				
			CVE ID : CVE-2021-31612						
	1		Operating System						
actions-semi									
ats2815_firm	nware	_							
N/A	07-Sep-21	6.1	The Bluetooth Classic implementation on Actions ATS2815 and ATS2819 chipsets does not properly handle the reception of multiple LMP_host_connection_req packets, allowing attackers in radio range to trigger a denial of service (deadlock) of the device via crafted LMP packets. Manual user intervention is required to restart the device and restore Bluetooth communication. CVE ID : CVE-2021-31785	https://www. actions- semi.com/ind ex.php?id=35 81&siteId=4	0-ACT-ATS2- 200921/2155				
N/A	07-Sep-21	6.1	The Bluetooth Classic Audio implementation on Actions ATS2815 and ATS2819 devices does not properly	https://www. actions- semi.com/ind ex.php?id=35	O-ACT-ATS2- 200921/2156				

CVSS Scoring Scale	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10
			П		£ 1 1 7 1					

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			handle a connection attempt from a host with the same BDAddress as the current connected BT host, allowing attackers to trigger a disconnection and deadlock of the device by connecting with a forged BDAddress that matches the original connected host. CVE ID : CVE-2021-31786	81&siteId=4	
ats2819p_fir	mware				
N/A	07-Sep-21	6.1	The Bluetooth Classic implementation on Actions ATS2815 and ATS2819 chipsets does not properly handle the reception of multiple LMP_host_connection_req packets, allowing attackers in radio range to trigger a denial of service (deadlock) of the device via crafted LMP packets. Manual user intervention is required to restart the device and restore Bluetooth communication. CVE ID : CVE-2021-31785	https://www. actions- semi.com/ind ex.php?id=35 81&siteId=4	O-ACT-ATS2- 200921/2157
N/A 07-Sep-21 6.1 CVSS Scoring Scale 0-1 1-2		The Bluetooth Classic Audio implementation on Actions ATS2815 and ATS2819 devices does not properly handle a connection attempt from a host with the same BDAddress as the current connected BT host, allowing attackers to trigger a disconnection and deadlock of the device by connecting	https://www. actions- semi.com/ind ex.php?id=35 81&siteId=4	O-ACT-ATS2- 200921/2158	

Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
		with a forged BDAddress that matches the original connected host.		
		CVE ID : CVE-2021-31786		
mware		I		
07-Sep-21	6.1	The Bluetooth Classic implementation on Actions ATS2815 and ATS2819 chipsets does not properly handle the reception of multiple LMP_host_connection_req packets, allowing attackers in radio range to trigger a denial of service (deadlock) of the device via crafted LMP packets. Manual user intervention is required to restart the device and restore Bluetooth communication. CVE ID : CVE-2021-31785	https://www. actions- semi.com/ind ex.php?id=35 81&siteId=4	O-ACT-ATS2- 200921/2159
07-Sep-21	6.1	The Bluetooth Classic Audio implementation on Actions ATS2815 and ATS2819 devices does not properly handle a connection attempt from a host with the same BDAddress as the current connected BT host, allowing attackers to trigger a disconnection and deadlock of the device by connecting with a forged BDAddress that matches the original connected host. CVE ID : CVE-2021-31786	https://www. actions- semi.com/ind ex.php?id=35 81&siteId=4	0-ACT-ATS2- 200921/2160
	07-Sep-21	• •	orderorderBDAddress that matches the original connected host.TWWATEO7-Sep-21The Bluetooth Classic implementation on Actions ATS2815 and ATS2819 chipsets does not properly handle the reception of multiple LMP_host_connection_req packets, allowing attackers in radio range to trigger a denial of service (deadlock) of the device via crafted LMP packets. Manual user intervention is required to restart the device and restore Bluetooth communication.07-Sep-216.1The Bluetooth Classic Audio implementation on Actions ATS2815 and ATS2819 devices does not properly handle a connection attempt from a host with the same BDAddress as the current connected BT host, allowing attackers to trigger a disconnection and deadlock of the device by connecting with a forged BDAddress that matches the original connected host.	orderwith a forged BDAddress that matches the original connected host.image: connected host.mwareCVE ID : CVE-2021-31786mwareThe Bluetooth Classic implementation on Actions ATS2815 and ATS2819 chipsets does not properly handle the reception of multiple LMP_host_connection_req packets, allowing attackers in radio range to trigger a denial of service (deadlock) of the device via crafted LMP packets. Manual user intervention is required to restart the device and restore Bluetooth Classic Audio implementation on Actions ATS2815 and ATS2819https://www. actions- semi.com/ind ex.php?id=35 81&siteld=407-Sep-216.1The Bluetooth Classic Audio implementation on Actions ATS2815 and ATS2819 devices does not properly handle a connection attempt from a host with the same BDAddress as the current connected BT host, allowing attackers to trigger a disconnection and deadlock of the device by connecting with a forged BDAddress that matches the original connected host.https://www.

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
N/A	07-Sep-21	6.1	The Bluetooth Classic implementation on Actions ATS2815 and ATS2819 chipsets does not properly handle the reception of multiple LMP_host_connection_req packets, allowing attackers in radio range to trigger a denial of service (deadlock) of the device via crafted LMP packets. Manual user intervention is required to restart the device and restore Bluetooth communication. CVE ID : CVE-2021-31785	https://www. actions- semi.com/ind ex.php?id=35 81&siteId=4	0-ACT-ATS2- 200921/2161
N/A	07-Sep-21	6.1	The Bluetooth Classic Audio implementation on Actions ATS2815 and ATS2819 devices does not properly handle a connection attempt from a host with the same BDAddress as the current connected BT host, allowing attackers to trigger a disconnection and deadlock of the device by connecting with a forged BDAddress that matches the original connected host. CVE ID : CVE-2021-31786	https://www. actions- semi.com/ind ex.php?id=35 81&siteId=4	0-ACT-ATS2- 200921/2162
ats2819_firmware					
N/A	07-Sep-21	6.1	The Bluetooth Classic implementation on Actions ATS2815 and ATS2819 chipsets does not properly handle the reception of multiple LMP_host_connection_req	https://www. actions- semi.com/ind ex.php?id=35 81&siteId=4	0-ACT-ATS2- 200921/2163
CVSS Scoring Sc	ale 0-1	1-2	2-3 3-4 4-5 5-6 Page 861 of 1474	6-7 7-8	8-9 9-10

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			packets, allowing attackers in radio range to trigger a denial of service (deadlock) of the device via crafted LMP packets. Manual user intervention is required to restart the device and restore Bluetooth communication. CVE ID : CVE-2021-31785		
N/A	07-Sep-21	6.1	The Bluetooth Classic Audio implementation on Actions ATS2815 and ATS2819 devices does not properly handle a connection attempt from a host with the same BDAddress as the current connected BT host, allowing attackers to trigger a disconnection and deadlock of the device by connecting with a forged BDAddress that matches the original connected host. CVE ID : CVE-2021-31786	https://www. actions- semi.com/ind ex.php?id=35 81&siteId=4	0-ACT-ATS2- 200921/2164
Amazon	I			I	I
kindle_firmw	vare				
Integer Overflow or Wraparoun d	01-Sep-21	9.3	Amazon Kindle e-reader prior to and including version 5.13.4 contains an Integer Overflow that leads to a Heap-Based Buffer Overflow in function CJBig2Image::expand() and results in a memory corruption that leads to code execution when parsing a crafted PDF book. CVE ID : CVE-2021-30354	N/A	O-AMA-KIND- 200921/2165
CVSS Scoring Sc	ale 0-1	1-2	2-3 3-4 4-5 5-6 Page 862 of 1474	6-7 7-8	8-9 9-10

Page 862 of 1474

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Improper Privilege Managemen t	01-Sep-21	9.3	Amazon Kindle e-reader prior to and including version 5.13.4 improperly manages privileges, allowing the framework user to elevate privileges to root. CVE ID : CVE-2021-30355	N/A	0-AMA-KIND- 200921/2166
Apple					•
ipados	1			1	1
Out-of- bounds Write	08-Sep-21	6.8	A stack overflow was addressed with improved input validation. This issue is fixed in iOS 14.7, macOS Big Sur 11.5, watchOS 7.6, tvOS 14.7, Security Update 2021- 005 Mojave, Security Update 2021-004 Catalina. Processing a maliciously crafted font file may lead to arbitrary code execution. CVE ID : CVE-2021-30759	https://supp ort.apple.com /en- us/HT21260 4, https://supp ort.apple.com /en- us/HT21260 5, https://supp ort.apple.com /en- us/HT21260 2, https://supp ort.apple.com /en- us/HT21260 3, https://supp ort.apple.com /en- us/HT21260 0, https://supp ort.apple.com /en- us/HT21260 1	O-APP-IPAD- 200921/2167
CVSS Scoring Sc	ale 0-1	1-2	2-3 3-4 4-5 5-6 Page 863 of 1474	6-7 7-8	8-9 9-10

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Improper Input Validation	08-Sep-21	4.3	An input validation issue was addressed with improved input validation. This issue is fixed in iOS 14.7, watchOS 7.6. A shortcut may be able to bypass Internet permission requirements. CVE ID : CVE-2021-30763	https://supp ort.apple.com /en- us/HT21260 5, https://supp ort.apple.com /en- us/HT21260 1	O-APP-IPAD- 200921/2168
N/A	08-Sep-21	6.8	Processing a maliciously crafted file may lead to arbitrary code execution. This issue is fixed in iOS 14.5 and iPadOS 14.5, watchOS 7.4, tvOS 14.5. This issue was addressed with improved checks. CVE ID : CVE-2021-30764	https://supp ort.apple.com /en- us/HT21231 7, https://supp ort.apple.com /en- us/HT21232 3, https://supp ort.apple.com /en- us/HT21232 4	O-APP-IPAD- 200921/2169
N/A	08-Sep-21	6.8	This issue was addressed with improved checks. This issue is fixed in iOS 14.7, Safari 14.1.2, macOS Big Sur 11.5, watchOS 7.6, tvOS 14.7. Processing maliciously crafted web content may lead to code execution. CVE ID : CVE-2021-30797	https://supp ort.apple.com /en- us/HT21260 6, https://supp ort.apple.com /en- us/HT21260 4, https://supp ort.apple.com /en- us/HT21260 5,	O-APP-IPAD- 200921/2170
CVSS Scoring Sc	ale 0-1	1-2	2-3 3-4 4-5 5-6 Page 864 of 1474	6-7 7-8	8-9 9-10

Page 864 of 1474

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
				https://supp ort.apple.com /en- us/HT21260 2, https://supp ort.apple.com /en- us/HT21260 1	
ipad_os					
Improper Authenticati on	08-Sep-21	5.8	A logic issue was addressed with improved restrictions. This issue is fixed in tvOS 14.6, iOS 14.6 and iPadOS 14.6, Safari 14.1.1, macOS Big Sur 11.4, watchOS 7.5. A malicious website may be able to access restricted ports on arbitrary servers. CVE ID : CVE-2021-30720	https://supp ort.apple.com /en- us/HT21252 9, https://supp ort.apple.com /en- us/HT21252 8, https://supp ort.apple.com /en- us/HT21253 4, https://supp ort.apple.com /en- us/HT21253 2, https://supp ort.apple.com /en- us/HT21253 3	O-APP-IPAD- 200921/2171
Improper Privilege Managemen	08-Sep-21	4.6	This issue was addressed with improved checks. This issue is fixed in tvOS 14.6,	https://supp ort.apple.com /en-	O-APP-IPAD- 200921/2172

CVSS Scoring Scale	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10
				0.05	6 4 4 - 4					

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
t			Security Update 2021-004 Mojave, iOS 14.6 and iPadOS 14.6, Security Update 2021- 003 Catalina, macOS Big Sur 11.4, watchOS 7.5. A local attacker may be able to elevate their privileges. CVE ID : CVE-2021-30724	us/HT21253 0, https://supp ort.apple.com /en- us/HT21253 1, https://supp ort.apple.com /en- us/HT21252 9, https://supp ort.apple.com /en- us/HT21252 8, https://supp ort.apple.com /en- us/HT21253 2, https://supp ort.apple.com /en- us/HT21253 3	
N/A	08-Sep-21	4.3	A logic issue was addressed with improved state management. This issue is fixed in macOS Big Sur 11.4, tvOS 14.6, watchOS 7.5, iOS 14.6 and iPadOS 14.6. A malicious application may be able to modify protected parts of the file system. CVE ID : CVE-2021-30727	https://supp ort.apple.com /en- us/HT21252 9, https://supp ort.apple.com /en- us/HT21252 8, https://supp ort.apple.com /en-	O-APP-IPAD- 200921/2173
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 & CVE ID	Patch	NCIIPC ID
				us/HT21253 2, https://supp ort.apple.com /en- us/HT21253 3	
N/A	08-Sep-21	5	A logic issue was addressed with improved restrictions. This issue is fixed in iOS 14.6 and iPadOS 14.6. A device may accept invalid activation results. CVE ID : CVE-2021-30729	https://supp ort.apple.com /en- us/HT21252 8	O-APP-IPAD- 200921/2174
Out-of- bounds Read	08-Sep-21	4.3	An out-of-bounds read was addressed with improved input validation. This issue is fixed in tvOS 14.6, iOS 14.6 and iPadOS 14.6, Security Update 2021-004 Catalina, Security Update 2021-005 Mojave, macOS Big Sur 11.4, watchOS 7.5. Processing a maliciously crafted font may result in the disclosure of process memory. CVE ID : CVE-2021-30733	https://supp ort.apple.com /en- us/HT21252 9, https://supp ort.apple.com /en- us/HT21252 8, https://supp ort.apple.com /en- us/HT21260 3, https://supp ort.apple.com /en- us/HT21260 0, https://supp ort.apple.com /en- us/HT21253 2,	O-APP-IPAD- 200921/2175

CVSS Scoring Scale

0-1

1-2

6-7

5-6

7-8

8-9

9-10

bounds Write08-Sep-216.814.0, Sharr 14.1.1, mactors big Sur 11.4, watchOS 7.5. Processing maliciously crafted web content may lead to arbitrary code execution./en- us/HT21253 2, https://supp ort.apple.com /en- us/HT21253 2, https://supp ort.apple.com /en- us/HT21253 2, https://supp ort.apple.com /en- us/HT21253 32009Buffer Copy without Checking Size of Input ('Classic08-Sep-219.3A buffer overflow was addressed with improved size validation. This issue is fixed in macOS Big Sur 11.4, tvOS 14.6, watchOS 7.5, iOS 14.6 and iPadOS 14.6. Anhttps://supp ort.apple.com /en- us/HT21252 9, https://supp ort.apple.com /en- us/HT21252 9, https://supp0-AP 2009	Weakness	Publish Date CVSS	CVSS Description & CVE ID	Patch	NCIIPC ID
Out-of- bounds08-Sep-216.8Multiple memory corruption issues were addressed with improved memory handling. This issue is fixed in tvOS 14.6, iOS 14.6 and iPadOS Sur 11.4, watchOS 7.5. Processing maliciously crafted web content may lead to arbitrary code execution.O-AP (en- us/HT21253 8, https://supp ort.apple.com /en- us/HT21253 4, https://supp ort.apple.com /en- us/HT21253 2, https://supp ort.apple.com /en- us/HT21253 2, https://supp ort.apple.com /en- us/HT21253 2, https://supp ort.apple.com /en- us/HT21253 3O-AP 2009Buffer Copy without Checking Size of Input (Classic08-Sep-219.3A buffer overflow was addressed with improved size validation. This issue is fixed in macOS Big Sur 11.4, vort.apple.com /en- us/HT21253 2, https://supp ort.apple.com /en- us/HT21253 2, https://supp ort.apple.com /en- us/HT21253 2, https://supp ort.apple.com /en- us/HT21253 2, https://supp ort.apple.com /en- us/HT21253 2, https://supp ort.apple.com /en- us/HT21253 2, https://supp ort.apple.com /en- us/HT21252 9, https://supp O-AP 2009				ort.apple.com /en- us/HT21253	
Buffer Copy withoutaddressed with improved size validation. This issue is fixed in macOS Big Sur 11.4,ort.apple.com /en- us/HT21252Size of Input ('Classic08-Sep-219.3tvOS 14.6, watchOS 7.5, iOS 	bounds	08-Sep-21 6.8	 issues were addressed with improved memory handling This issue is fixed in tvOS 14.6, iOS 14.6 and iPadOS 6.8 14.6, Safari 14.1.1, macOS B Sur 11.4, watchOS 7.5. Processing maliciously crafted web content may lead to arbitrary code execution. 	ort.apple.com /en- us/HT21252 9, https://supp ort.apple.com /en- us/HT21252 8, https://supp ort.apple.com /en- us/HT21253 4, https://supp ort.apple.com /en- us/HT21253 2, https://supp ort.apple.com /en- us/HT21253	0-APP-IPAD- 200921/2176
Overflow')execute arbitrary code with kernel privileges./en- us/HT21252 8,	without Checking Size of Input ('Classic Buffer	08-Sep-21 9.3	 addressed with improved size validation. This issue is fixed in macOS Big Sur 11.4, tvOS 14.6, watchOS 7.5, iOS 14.6 and iPadOS 14.6. An application may be able to execute arbitrary code with 	ort.apple.com /en- us/HT21252 9, https://supp ort.apple.com /en- us/HT21252	O-APP-IPAD- 200921/2177

Page 868 of 1474

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2021-30736	https://supp ort.apple.com /en- us/HT21253 2, https://supp ort.apple.com /en- us/HT21253 3	
Out-of- bounds Write	08-Sep-21	6.8	A memory corruption issue in the ASN.1 decoder was addressed by removing the vulnerable code. This issue is fixed in tvOS 14.6, Security Update 2021-004 Mojave, iOS 14.6 and iPadOS 14.6, iOS 12.5.4, Security Update 2021- 003 Catalina, macOS Big Sur 11.4, watchOS 7.5. Processing a maliciously crafted certificate may lead to arbitrary code execution. CVE ID : CVE-2021-30737	https://supp ort.apple.com /en- us/HT21253 0, https://supp ort.apple.com /en- us/HT21253 1, https://supp ort.apple.com /en- us/HT21252 9, https://supp ort.apple.com /en- us/HT21252 8, https://supp ort.apple.com /en- us/HT21254 8, https://supp ort.apple.com /en- us/HT21254 8, https://supp ort.apple.com /en- us/HT21253 2	O-APP-IPAD- 200921/2178
CVSS Scoring Sc	ale 0-1	1-2	2-3 3-4 4-5 5-6 Page 869 of 1474	6-7 7-8	8-9 9-10

Page 869 of 1474

Weakness	Publish Date	CVSS	Desc	riptior	n & CVE I	D	Pat	ch	NCI	PC ID
N/A	08-Sep-21	9.3	A logic iss with impr This issue Big Sur 11 watchOS 7 iPadOS 14 applicatio execute an kernel pri CVE ID : C	roved e is fix 1.4, tv 7.5, iO 4.6. A on may rbitra ivilege	validati ed in ma OS 14.6 S 14.6 a malicion y be abl ry code es.	on. acOS and is e to with	https:// ort.app /en- us/HT2 9, https:// ort.app /en- us/HT2 8, https:// ort.app /en- us/HT2 2, https:// ort.app /en- us/HT2 3	le.com 21252 /supp le.com 21252 /supp le.com 21253 /supp le.com	0-APP 20092	-IPAD- 1/2179
Use After Free	08-Sep-21	5.8	A use after addressed memory r issue is fix iPadOS 14 malicious message r unexpecter modification termination CVE ID : C	l with nanag ked in 4.6. Pr ly cra nay le ed me ion or on.	improv gement. iOS 14. ocessin fted ma ead to mory applica	ved This 6 and g a il ttion	https:// ort.app /en- us/HT2 8	le.com	0-APP 20092	-IPAD- 1/2180
Uncontrolle d Resource Consumptio n	08-Sep-21	6.8	A memory was addre improved This issue and iPadC a maliciou file may le code exec	essed mem is fix)S 14. Isly cr ead to	with ory han ed in iO 5. Proce rafted an arbitra	dling. S 14.5 essing udio	https:// ort.app /en- us/HT2 7	le.com	0-APP 20092	-IPAD- 1/2181
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 & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2021-30742		
Out-of- bounds Write	08-Sep-21	6.8	An out-of-bounds write was addressed with improved input validation. This issue is fixed in iOS 14.5 and iPadOS 14.5, watchOS 7.4, Security Update 2021-003 Catalina, tvOS 14.5, macOS Big Sur 11.3. Processing a maliciously crafted image may lead to arbitrary code execution. CVE ID : CVE-2021-30743	https://supp ort.apple.com /en- us/HT21253 0, https://supp ort.apple.com /en- us/HT21231 7, https://supp ort.apple.com /en- us/HT21232 5, https://supp ort.apple.com /en- us/HT21232 3, https://supp ort.apple.com /en- us/HT21232 3, https://supp ort.apple.com /en- us/HT21232 3,	O-APP-IPAD- 200921/2182
iphone_os	Γ				
N/A	02-Sep-21	4	Microsoft Edge for iOS Spoofing Vulnerability CVE ID : CVE-2021-38642	https://porta l.msrc.micros oft.com/en- US/security- guidance/adv isory/CVE- 2021-38642	O-APP-IPHO- 200921/2183
Improper Authenticati on	08-Sep-21	5.8	A logic issue was addressed with improved restrictions. This issue is fixed in tvOS 14.6, iOS 14.6 and iPadOS 14.6, Safari 14.1.1, macOS Big	https://supp ort.apple.com /en- us/HT21252 9,	O-APP-IPHO- 200921/2184
Authenticati		5.8	with improved restrictions. This issue is fixed in tvOS 14.6, iOS 14.6 and iPadOS	ort.apple.com /en- us/HT21252	

Improper t08-Sep-214.6Sur 11.4, watchOS 7.5. A malicious website may be able to access restricted ports on arbitrary servers. CVE ID : CVE-2021-30720https://supp ort.apple.com /en- us/HT21223 4, https://supp ort.apple.com /en- us/HT21253 2, https://supp ort.apple.com /en- us/HT21253 3Improper t08-Sep-214.6Fris issue was addressed with improved checks. This issue is fixed in tVoS 14.6, Security Update 2021-004 (Pa- us/HT21253 (Pa- us/HT21253 (Pa- us/HT21253 (Pa- us/HT21253 (Pa- us/HT21253 (Pa- us/HT21253 (Pa- us/HT21253 (Pa- us/HT21253 (Pa- us/HT21253 (Pa- us/HT21253 (Pa- us/HT21253 (Pa- us/HT21253 (Pa- us/HT21253 (Pa- us/HT21253 (Pa- us/HT21253 (Pa- us/HT21253 (Pa- us/HT21253 (Pa- us/HT21253 (Pa- us/HT21253 (Pa- us/HT21252 (Pa- Us/HT21252 (Pa- Us/HT21252 (Pa- Us/HT21252 	Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Improper Privilege ManagemenName Nesser-21Name Nesse				malicious website may be able to access restricted ports on arbitrary servers.	ort.apple.com /en- us/HT21252 8, https://supp ort.apple.com /en- us/HT21253 4, https://supp ort.apple.com /en- us/HT21253 2, https://supp ort.apple.com /en- us/HT21253	
	Privilege Managemen	08-Sep-21	4.6	with improved checks. This issue is fixed in tvOS 14.6, Security Update 2021-004 Mojave, iOS 14.6 and iPadOS 14.6, Security Update 2021- 003 Catalina, macOS Big Sur 11.4, watchOS 7.5. A local attacker may be able to elevate their privileges.	ort.apple.com /en- us/HT21253 0, https://supp ort.apple.com /en- us/HT21253 1, https://supp ort.apple.com /en- us/HT21252 9, https://supp ort.apple.com /en- us/HT21252	

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
				https://supp ort.apple.com /en- us/HT21253 2, https://supp ort.apple.com /en- us/HT21253 3	
N/A	08-Sep-21	4.3	A logic issue was addressed with improved state management. This issue is fixed in macOS Big Sur 11.4, tvOS 14.6, watchOS 7.5, iOS 14.6 and iPadOS 14.6. A malicious application may be able to modify protected parts of the file system. CVE ID : CVE-2021-30727	https://supp ort.apple.com /en- us/HT21252 9, https://supp ort.apple.com /en- us/HT21252 8, https://supp ort.apple.com /en- us/HT21253 2, https://supp ort.apple.com /en- us/HT21253 3	O-APP-IPHO- 200921/2186
N/A	08-Sep-21	5	A logic issue was addressed with improved restrictions. This issue is fixed in iOS 14.6 and iPadOS 14.6. A device may accept invalid activation results. CVE ID : CVE-2021-30729	https://supp ort.apple.com /en- us/HT21252 8	O-APP-IPHO- 200921/2187
Out-of- bounds	08-Sep-21	4.3	An out-of-bounds read was addressed with improved	https://supp ort.apple.com	O-APP-IPHO- 200921/2188

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Read			input validation. This issue is fixed in tvOS 14.6, iOS 14.6 and iPadOS 14.6, Security Update 2021-004 Catalina, Security Update 2021-005 Mojave, macOS Big Sur 11.4, watchOS 7.5. Processing a maliciously crafted font may result in the disclosure of process memory. CVE ID : CVE-2021-30733	/en- us/HT21252 9, https://supp ort.apple.com /en- us/HT21252 8, https://supp ort.apple.com /en- us/HT21260 3, https://supp ort.apple.com /en- us/HT21260 0, https://supp ort.apple.com /en- us/HT21253 2, https://supp ort.apple.com /en- us/HT21253 3	
Out-of- bounds Write	08-Sep-21	6.8	Multiple memory corruption issues were addressed with improved memory handling. This issue is fixed in tvOS 14.6, iOS 14.6 and iPadOS 14.6, Safari 14.1.1, macOS Big Sur 11.4, watchOS 7.5. Processing maliciously crafted web content may lead to arbitrary code execution. CVE ID : CVE-2021-30734	https://supp ort.apple.com /en- us/HT21252 9, https://supp ort.apple.com /en- us/HT21252 8, https://supp ort.apple.com	O-APP-IPHO- 200921/2189
CVSS Scoring Sc	ale 0-1	1-2	2-3 3-4 4-5 5-6	6-7 7-8	8-9 9-10

Page 874 of 1474

Size of Input ('Classic Buffer Overflow')08-Sep-219.314.6 and iPadOS 14.6. An application may be able to execute arbitrary code with kernel privileges.https://supp ort.apple.com /en- us/HT21253 2, https://supp ort.apple.com /en- us/HT21253 3200921/219Out-of- bounds Write08-Sep-216.8A memory corruption issue in the ASN.1 decoder was addressed by removing the vulnerable code. This issue is fixed in tvOS 14.6, Securityhttps://supp ort.apple.com /en- us/HT21253 0,0-APP-IPHO- 200921/219	Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')08-Sep-219.3A buffer overflow was addressed with improved size validation. This issue is fixed in macOS Big Sur 11.4, tvOS 14.6, watchOS 7.5, iOS 14.6 and iPadOS 14.6. An application may be able to execute arbitrary code with kernel privileges.0-APP-IPHO- 200921/219Out-of- bounds08-Sep-216.8A memory corruption issue in the ASN.1 decoder was addressed by removing the vulnerable code. This issue is fixed in tvOS 14.6, Securityhttps://supp ort.apple.com /en- us/HT21253 2, https://supp ort.apple.com /en- us/HT21253 30-APP-IPHO- 200921/219					us/HT21253 4, https://supp ort.apple.com /en- us/HT21253 2, https://supp ort.apple.com /en- us/HT21253	
Out-of- bounds08-Sep-216.8in the ASN.1 decoder was addressed by removing the vulnerable code. This issue is fixed in tvOS 14.6, Securityort.apple.com (en- us/HT212530-APP-IPHO- 200921/219	without Checking Size of Input ('Classic Buffer	08-Sep-21	9.3	addressed with improved size validation. This issue is fixed in macOS Big Sur 11.4, tvOS 14.6, watchOS 7.5, iOS 14.6 and iPadOS 14.6. An application may be able to execute arbitrary code with kernel privileges.	ort.apple.com /en- us/HT21252 9, https://supp ort.apple.com /en- us/HT21252 8, https://supp ort.apple.com /en- us/HT21253 2, https://supp ort.apple.com /en- us/HT21253	O-APP-IPHO- 200921/2190
Update 2021-004 Mojave, iOS https://supp 14.6 and iPadOS 14.6, iOS ort.apple.com CVSS Scoring Scale 0-1 1-2 2-3 3-4 4-5 5-6 6-7 7-8 8-9 9-10	bounds Write		6.8	in the ASN.1 decoder was addressed by removing the vulnerable code. This issue is fixed in tvOS 14.6, Security Update 2021-004 Mojave, iOS 14.6 and iPadOS 14.6, iOS	ort.apple.com /en- us/HT21253 0, https://supp	O-APP-IPHO- 200921/2191

Weakness	Publish Date	CVSS	D	escriptio	n & CVE I	D	Ра	tch	NCI	PC ID
			003 Ca 11.4, w a malic certific arbitra	talina, n vatchOS ciously c cate may ry code		g Sur cessing on.	/en- us/HT 9, https:/ ort.app /en- us/HT 8, https:/ ort.app /en- us/HT 8, https:/	2/supp ole.com 21252 2/supp ole.com 21252 2/supp ole.com 21254 2/supp ole.com		
N/A	08-Sep-21	9.3	with in This is Big Sur watch(iPadOS applica execute kernel	nproved sue is fix - 11.4, tw DS 7.5, i(5 14.6. A ation ma e arbitra privileg	as addre validati ced in ma cOS 14.6, DS 14.6 a maliciou y be able ry code es. 2021-30	on. acOS and is e to with	/en- us/HT 9, https:/ ort.app /en- us/HT 8, https:/ ort.app /en- us/HT 2, https:/	ole.com 21252 7/supp ole.com 21252 7/supp ole.com 21253		-IPHO- 1/2192
CVSS Scoring Sc	ale 0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10

Page 876 of 1474

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
				/en- us/HT21253 3	
Use After Free	08-Sep-21	5.8	A use after free issue was addressed with improved memory management. This issue is fixed in iOS 14.6 and iPadOS 14.6. Processing a maliciously crafted mail message may lead to unexpected memory modification or application termination. CVE ID : CVE-2021-30741	https://supp ort.apple.com /en- us/HT21252 8	O-APP-IPHO- 200921/2193
Uncontrolle d Resource Consumptio n	08-Sep-21	6.8	A memory consumption issue was addressed with improved memory handling. This issue is fixed in iOS 14.5 and iPadOS 14.5. Processing a maliciously crafted audio file may lead to arbitrary code execution. CVE ID : CVE-2021-30742	https://supp ort.apple.com /en- us/HT21231 7	O-APP-IPHO- 200921/2194
Out-of- bounds Write	08-Sep-21	6.8	An out-of-bounds write was addressed with improved input validation. This issue is fixed in iOS 14.5 and iPadOS 14.5, watchOS 7.4, Security Update 2021-003 Catalina, tvOS 14.5, macOS Big Sur 11.3. Processing a maliciously crafted image may lead to arbitrary code execution. CVE ID : CVE-2021-30743	https://supp ort.apple.com /en- us/HT21253 0, https://supp ort.apple.com /en- us/HT21231 7, https://supp ort.apple.com /en- us/HT21232 5, https://supp	O-APP-IPHO- 200921/2195

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
				ort.apple.com /en- us/HT21232 3, https://supp ort.apple.com /en- us/HT21232 4 https://supp	
Access of Resource Using Incompatibl e Type ('Type Confusion')	08-Sep-21	6.8	A type confusion issue was addressed with improved state handling. This issue is fixed in iOS 14.7, Safari 14.1.2, macOS Big Sur 11.5, watchOS 7.6, tvOS 14.7. Processing maliciously crafted web content may lead to arbitrary code execution. CVE ID : CVE-2021-30758	nttps://supp ort.apple.com /en- us/HT21260 6, https://supp ort.apple.com /en- us/HT21260 4, https://supp ort.apple.com /en- us/HT21260 5, https://supp ort.apple.com /en- us/HT21260 2, https://supp ort.apple.com /en- us/HT21260 1	0-APP-IPHO- 200921/2196
Out-of- bounds Write	08-Sep-21	6.8	A stack overflow was addressed with improved input validation. This issue is fixed in iOS 14.7, macOS Big Sur 11.5, watchOS 7.6, tvOS 14.7, Security Update 2021-	https://supp ort.apple.com /en- us/HT21260 4, https://supp	O-APP-IPHO- 200921/2197
CVSS Scoring Sc	ale 0-1	1-2	2-3 3-4 4-5 5-6 Page 878 of 1474	6-7 7-8	8-9 9-10

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			005 Mojave, Security Update 2021-004 Catalina. Processing a maliciously crafted font file may lead to arbitrary code execution. CVE ID : CVE-2021-30759	ort.apple.com /en- us/HT21260 5, https://supp ort.apple.com /en- us/HT21260 2, https://supp ort.apple.com /en- us/HT21260 3, https://supp ort.apple.com /en- us/HT21260 0, https://supp ort.apple.com /en- us/HT21260 1	
Out-of- bounds Write	08-Sep-21	6.8	A memory corruption issue was addressed with improved state management. This issue is fixed in iOS 12.5.4. Processing maliciously crafted web content may lead to arbitrary code execution. Apple is aware of a report that this issue may have been actively exploited CVE ID : CVE-2021-30761	https://supp ort.apple.com /en- us/HT21254 8	O-APP-IPHO- 200921/2198
Use After Free	08-Sep-21	6.8	A use after free issue was addressed with improved memory management. This	https://supp ort.apple.com /en-	O-APP-IPHO- 200921/2199

CVSS Scoring Scale	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10
erse scenng scale	v 1			J 1	1.5	50	0,	, 0	0.5	<u> </u>
Page 870 of 1474										

Improper		issue is fixed in iOS 12.5.4. Processing maliciously crafted web content may lead to arbitrary code execution. Apple is aware of a report that this issue may have been actively exploited CVE ID : CVE-2021-30762	us/HT21254 8	
Improper				1
Input 08-Sep-21 Validation	4.3	An input validation issue was addressed with improved input validation. This issue is fixed in iOS 14.7, watchOS 7.6. A shortcut may be able to bypass Internet permission requirements. CVE ID : CVE-2021-30763	https://supp ort.apple.com /en- us/HT21260 5, https://supp ort.apple.com /en- us/HT21260 1	O-APP-IPHO- 200921/2200
N/A 08-Sep-21	6.8	Processing a maliciously crafted file may lead to arbitrary code execution. This issue is fixed in iOS 14.5 and iPadOS 14.5, watchOS 7.4, tvOS 14.5. This issue was addressed with improved checks. CVE ID : CVE-2021-30764	https://supp ort.apple.com /en- us/HT21231 7, https://supp ort.apple.com /en- us/HT21232 3, https://supp ort.apple.com /en- us/HT21232 4	O-APP-IPHO- 200921/2201
N/A 08-Sep-21	6.8	This issue was addressed with improved checks. This issue is fixed in iOS 14.7, Safari 14.1.2, macOS Big Sur 11.5, watchOS 7.6, tvOS 14.7. Processing maliciously	https://supp ort.apple.com /en- us/HT21260 6, https://supp	O-APP-IPHO- 200921/2202

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
	Publish Date	CVSS	Description & CVE ID crafted web content may lead to code execution. CVE ID : CVE-2021-30797 A logic issue was addressed with improved state management. This issue is	Patch ort.apple.com /en- us/HT21260 4, https://supp ort.apple.com /en- us/HT21260 5, https://supp ort.apple.com /en- us/HT21260 2, https://supp ort.apple.com /en- us/HT21260 1 https://supp ort.apple.com /en- us/HT21260 5, https://supp	NCIIPC ID
Exposure of Resource to Wrong Sphere	08-Sep-21	7.8	fixed in iOS 14.7, macOS Big Sur 11.5, watchOS 7.6. A malicious application may be able to bypass certain Privacy preferences. CVE ID : CVE-2021-30798	https://supp ort.apple.com /en- us/HT21260 2, https://supp ort.apple.com /en- us/HT21260 1	O-APP-IPHO- 200921/2203
macos					
Out-of- bounds Write	02-Sep-21	6.8	Acrobat Reader DC versions versions 2020.013.20074 (and earlier), 2020.001.30018 (and	https://helpx .adobe.com/s ecurity/prod ucts/acrobat/	O-APP-MACO- 200921/2204
CVSS Scoring Sc	ale 0-1	1-2	2-3 3-4 4-5 5-6	6-7 7-8	8-9 9-10

Page 881 of 1474

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			earlier) and 2017.011.30188 (and earlier) are affected by an Out-of-bounds Write vulnerability in the CoolType library. 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-2021-21086	apsb21- 09.html	
Creation of Temporary File in Directory with Insecure Permissions	08-Sep-21	6.9	Adobe Genuine Services version 7.1 (and earlier) is affected by an Insecure file permission vulnerability during installation process. A local authenticated attacker could leverage this vulnerability to achieve privilege escalation in the context of the current user. CVE ID : CVE-2021-28568	https://helpx .adobe.com/s ecurity/prod ucts/integrity _service/apsb 21-27.html	O-APP-MACO- 200921/2205
Access of Resource Using Incompatibl e Type ('Type Confusion')	08-Sep-21	6.8	A type confusion issue was addressed with improved state handling. This issue is fixed in iOS 14.7, Safari 14.1.2, macOS Big Sur 11.5, watchOS 7.6, tvOS 14.7. Processing maliciously crafted web content may lead to arbitrary code execution. CVE ID : CVE-2021-30758	https://supp ort.apple.com /en- us/HT21260 6, https://supp ort.apple.com /en- us/HT21260 4, https://supp ort.apple.com /en- us/HT21260	O-APP-MACO- 200921/2206

CVSS Scoring Scale

0-1

1-2

5-6

6-7

7-8

8-9

9-10

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
				5, https://supp ort.apple.com /en- us/HT21260 2, https://supp ort.apple.com /en- us/HT21260 1	
Out-of- bounds Write	08-Sep-21	6.8	A stack overflow was addressed with improved input validation. This issue is fixed in iOS 14.7, macOS Big Sur 11.5, watchOS 7.6, tvOS 14.7, Security Update 2021- 005 Mojave, Security Update 2021-004 Catalina. Processing a maliciously crafted font file may lead to arbitrary code execution. CVE ID : CVE-2021-30759	https://supp ort.apple.com /en- us/HT21260 4, https://supp ort.apple.com /en- us/HT21260 5, https://supp ort.apple.com /en- us/HT21260 2, https://supp ort.apple.com /en- us/HT21260 3, https://supp ort.apple.com /en- us/HT21260 0, https://supp ort.apple.com /en- us/HT21260 0, https://supp ort.apple.com /en- us/HT21260	O-APP-MACO- 200921/2207
CVSS Scoring Sc	cale 0-1	1-2	2-3 3-4 4-5 5-6	6-7 7-8	8-9 9-10

Page 883 of 1474

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
				1	
N/A	08-Sep-21	6.8	This issue was addressed with improved checks. This issue is fixed in iOS 14.7, Safari 14.1.2, macOS Big Sur 11.5, watchOS 7.6, tvOS 14.7. Processing maliciously crafted web content may lead to code execution. CVE ID : CVE-2021-30797	https://supp ort.apple.com /en- us/HT21260 6, https://supp ort.apple.com /en- us/HT21260 4, https://supp ort.apple.com /en- us/HT21260 5, https://supp ort.apple.com /en- us/HT21260 2, https://supp ort.apple.com /en- us/HT21260 1	O-APP-MACO- 200921/2208
Exposure of Resource to Wrong Sphere	08-Sep-21	7.8	A logic issue was addressed with improved state management. This issue is fixed in iOS 14.7, macOS Big Sur 11.5, watchOS 7.6. A malicious application may be able to bypass certain Privacy preferences. CVE ID : CVE-2021-30798	https://supp ort.apple.com /en- us/HT21260 5, https://supp ort.apple.com /en- us/HT21260 2, https://supp ort.apple.com /en- us/HT21260	O-APP-MACO- 200921/2209
CVSS Scoring Sc	ale 0-1	1-2	2-3 3-4 4-5 5-6	6-7 7-8	8-9 9-10

Page 884 of 1474

				1	
Loop with Unreachable Exit Condition ('Infinite Loop')	07-Sep-21	4.3	A vulnerability affecting F- Secure Antivirus engine was discovered whereby scanning WIM archive file can lead to denial-of-service (infinite loop and freezes AV engine scanner). The vulnerability can be exploit remotely by an attacker. A successful attack will result in Denial-of-Service of the Anti-Virus engine. CVE ID : CVE-2021-33599	https://www. f- secure.com/e n/business/p rograms/vuln erability- reward- program/hall -of-fame, https://www. f- secure.com/e n/business/s upport-and- downloads/s ecurity- advisories/cv e-2021- 33599	O-APP-MACO- 200921/2210
Out-of- bounds Write	01-Sep-21	9.3	Adobe Photoshop versions 21.2.10 (and earlier) and 22.4.3 (and earlier) are affected by a heap-based buffer overflow 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 file. CVE ID : CVE-2021-36065	https://helpx .adobe.com/s ecurity/prod ucts/photosh op/apsb21- 68.html	O-APP-MACO- 200921/2211
Out-of- bounds Write	01-Sep-21	9.3	Adobe Photoshop versions 21.2.10 (and earlier) and 22.4.3 (and earlier) are affected by an out-of-bounds write vulnerability that could result in arbitrary code	https://helpx .adobe.com/s ecurity/prod ucts/photosh op/apsb21- 68.html	O-APP-MACO- 200921/2212

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			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-2021-36066		
mac_os					
Improper Authenticati on	08-Sep-21	5.8	A logic issue was addressed with improved restrictions. This issue is fixed in tvOS 14.6, iOS 14.6 and iPadOS 14.6, Safari 14.1.1, macOS Big Sur 11.4, watchOS 7.5. A malicious website may be able to access restricted ports on arbitrary servers. CVE ID : CVE-2021-30720	https://supp ort.apple.com /en- us/HT21252 9, https://supp ort.apple.com /en- us/HT21252 8, https://supp ort.apple.com /en- us/HT21253 4, https://supp ort.apple.com /en- us/HT21253 2, https://supp ort.apple.com /en- us/HT21253 3	O-APP-MAC 200921/2213
Improper Privilege Managemen t	08-Sep-21	4.6	This issue was addressed with improved checks. This issue is fixed in tvOS 14.6, Security Update 2021-004 Mojave, iOS 14.6 and iPadOS 14.6, Security Update 2021- 003 Catalina, macOS Big Sur	https://supp ort.apple.com /en- us/HT21253 0, https://supp ort.apple.com	O-APP-MAC 200921/2214
CVSS Scoring Sca	ale 0-1	1-2	2-3 3-4 4-5 5-6	6-7 7-8	8-9 9-10

Page 886 of 1474

11.4, watchOS 7.5. A local/en- us/HT21253attacker may be able tous/HT21253elevate their privileges.1,CVE ID : CVE-2021-30724https://supp ort.apple.com	
/en- us/HT21252 9, https://supp ort.apple.com /en- us/HT21252 8, https://supp ort.apple.com /en- us/HT21253 2, https://supp ort.apple.com /en- us/HT21253 3	
N/A 08-Sep-21 4.3 A logic issue was addressed with improved state management. This issue is fixed in macOS Big Sur 11.4, tvOS 14.6, watchOS 7.5, iOS 14.6 and iPadOS 14.6. A malicious application may be able to modify protected parts of the file system. CVE ID : CVE-2021-30727 https://supp ort.apple.com /en- us/HT21252 8, https://supp ort.apple.com /en- us/HT21253 2, https://supp ort.apple.com /en- us/HT21253 2, https://supp	_
https://supp ort.apple.com	

3-4 4-5 Page 887 of 1474

Weakness F	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
				/en- us/HT21253 3 https://supp	
Out-of- bounds C Read	08-Sep-21	4.3	An out-of-bounds read was addressed with improved input validation. This issue is fixed in tvOS 14.6, iOS 14.6 and iPadOS 14.6, Security Update 2021-004 Catalina, Security Update 2021-005 Mojave, macOS Big Sur 11.4, watchOS 7.5. Processing a maliciously crafted font may result in the disclosure of process memory. CVE ID : CVE-2021-30733	nttps://supp ort.apple.com /en- us/HT21252 9, https://supp ort.apple.com /en- us/HT21252 8, https://supp ort.apple.com /en- us/HT21260 3, https://supp ort.apple.com /en- us/HT21260 0, https://supp ort.apple.com /en- us/HT21253 2, https://supp ort.apple.com /en- us/HT21253 3	0-APP-MAC 200921/2216
Out-of- bounds 0 Write	08-Sep-21	6.8	Multiple memory corruption issues were addressed with improved memory handling. This issue is fixed in tvOS 14.6, iOS 14.6 and iPadOS 14.6, Safari 14.1.1, macOS Big Sur 11.4, watchOS 7.5.	https://supp ort.apple.com /en- us/HT21252 9, https://supp ort.apple.com	O-APP-MAC 200921/2217
CVSS Scoring Scale	e 0-1	1-2	2-3 3-4 4-5 5-6	6-7 7-8	8-9 9-10

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Processing maliciously crafted web content may lead to arbitrary code execution. CVE ID : CVE-2021-30734	/en- us/HT21252 8, https://supp ort.apple.com /en- us/HT21253 4, https://supp ort.apple.com /en- us/HT21253 2, https://supp ort.apple.com /en- us/HT21253 3	
Out-of- bounds Write	08-Sep-21	9.3	A malicious application may be able to execute arbitrary code with kernel privileges. This issue is fixed in macOS Big Sur 11.4, Security Update 2021-003 Catalina, Security Update 2021-004 Mojave. An out-of-bounds write issue was addressed with improved bounds checking. CVE ID : CVE-2021-30735	https://supp ort.apple.com /en- us/HT21253 0, https://supp ort.apple.com /en- us/HT21253 1, https://supp ort.apple.com /en- us/HT21252 9	O-APP-MAC 200921/2218
Buffer Copy without Checking Size of Input ('Classic Buffer CVSS Scoring Sc	08-Sep-21	9.3	A buffer overflow was addressed with improved size validation. This issue is fixed in macOS Big Sur 11.4, tvOS 14.6, watchOS 7.5, iOS 14.6 and iPadOS 14.6. An application may be able to 2-3 3-4 4-5 5-6	https://supp ort.apple.com /en- us/HT21252 9, https://supp ort.apple.com	0-APP-MAC 200921/2219 8-9 9-10

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Overflow')			execute arbitrary code with kernel privileges. CVE ID : CVE-2021-30736	/en- us/HT21252 8, https://supp ort.apple.com /en- us/HT21253 2, https://supp ort.apple.com /en- us/HT21253 3	
Out-of- bounds Write	08-Sep-21	6.8	A memory corruption issue in the ASN.1 decoder was addressed by removing the vulnerable code. This issue is fixed in tvOS 14.6, Security Update 2021-004 Mojave, iOS 14.6 and iPadOS 14.6, iOS 12.5.4, Security Update 2021- 003 Catalina, macOS Big Sur 11.4, watchOS 7.5. Processing a maliciously crafted certificate may lead to arbitrary code execution. CVE ID : CVE-2021-30737	https://supp ort.apple.com /en- us/HT21253 0, https://supp ort.apple.com /en- us/HT21253 1, https://supp ort.apple.com /en- us/HT21252 9, https://supp ort.apple.com /en- us/HT21252 8, https://supp ort.apple.com /en- us/HT21254 8, https://supp ort.apple.com	O-APP-MAC 200921/2220
CVSS Scoring Sc	ale 0-1	1-2	2-3 3-4 4-5 5-6 Page 890 of 1/7/	6-7 7-8	8-9 9-10

Page 890 of 1474

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
				/en- us/HT21253 2	
N/A	08-Sep-21	2.1	A malicious application may be able to overwrite arbitrary files. This issue is fixed in macOS Big Sur 11.4, Security Update 2021-004 Mojave. An issue with path validation logic for hardlinks was addressed with improved path sanitization. CVE ID : CVE-2021-30738	https://supp ort.apple.com /en- us/HT21253 1, https://supp ort.apple.com /en- us/HT21252 9	0-APP-MAC 200921/2221
Out-of- bounds Write	08-Sep-21	4.6	A local attacker may be able to elevate their privileges. This issue is fixed in macOS Big Sur 11.4, Security Update 2021-003 Catalina, Security Update 2021-004 Mojave. A memory corruption issue was addressed with improved validation. CVE ID : CVE-2021-30739	https://supp ort.apple.com /en- us/HT21253 0, https://supp ort.apple.com /en- us/HT21253 1, https://supp ort.apple.com /en- us/HT21252 9	O-APP-MAC 200921/2222
N/A	08-Sep-21	9.3	A logic issue was addressed with improved validation. This issue is fixed in macOS Big Sur 11.4, tvOS 14.6, watchOS 7.5, iOS 14.6 and iPadOS 14.6. A malicious application may be able to execute arbitrary code with kernel privileges. CVE ID : CVE-2021-30740	https://supp ort.apple.com /en- us/HT21252 9, https://supp ort.apple.com /en- us/HT21252 8, https://supp	O-APP-MAC 200921/2223
CVSS Scoring Sc	cale 0-1	1-2	2-3 3-4 4-5 5-6	6-7 7-8	8-9 9-10

Page 891 of 1474

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
				ort.apple.com /en- us/HT21253 2, https://supp ort.apple.com /en- us/HT21253 3 https://supp	
Out-of- bounds Write	08-Sep-21	6.8	An out-of-bounds write was addressed with improved input validation. This issue is fixed in iOS 14.5 and iPadOS 14.5, watchOS 7.4, Security Update 2021-003 Catalina, tvOS 14.5, macOS Big Sur 11.3. Processing a maliciously crafted image may lead to arbitrary code execution. CVE ID : CVE-2021-30743	nttps://supp ort.apple.com /en- us/HT21253 0, https://supp ort.apple.com /en- us/HT21231 7, https://supp ort.apple.com /en- us/HT21232 5, https://supp ort.apple.com /en- us/HT21232 3, https://supp ort.apple.com /en- us/HT21232 4	O-APP-MAC 200921/2224
mac_os_x				L	L
Improper Privilege Managemen t	08-Sep-21	4.6	This issue was addressed with improved checks. This issue is fixed in tvOS 14.6, Security Update 2021-004	https://supp ort.apple.com /en- us/HT21253	O-APP-MAC 200921/2225
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 & CVE ID	Patch	NCIIPC ID
			Mojave, iOS 14.6 and iPadOS 14.6, Security Update 2021- 003 Catalina, macOS Big Sur 11.4, watchOS 7.5. A local attacker may be able to elevate their privileges. CVE ID : CVE-2021-30724	0, https://supp ort.apple.com /en- us/HT21253 1, https://supp ort.apple.com /en- us/HT21252 9, https://supp ort.apple.com /en- us/HT21252 8, https://supp ort.apple.com /en- us/HT21253 2, https://supp ort.apple.com /en- us/HT21253 3	
Out-of- bounds Read	08-Sep-21	4.3	An out-of-bounds read was addressed with improved input validation. This issue is fixed in tvOS 14.6, iOS 14.6 and iPadOS 14.6, Security Update 2021-004 Catalina, Security Update 2021-005 Mojave, macOS Big Sur 11.4, watchOS 7.5. Processing a maliciously crafted font may result in the disclosure of process memory. CVE ID : CVE-2021-30733	https://supp ort.apple.com /en- us/HT21252 9, https://supp ort.apple.com /en- us/HT21252 8, https://supp ort.apple.com /en- us/HT21260	O-APP-MAC 200921/2226
CVSS Scoring Sc	ale 0-1	1-2	2-3 3-4 4-5 5-6	6-7 7-8	8-9 9-10

Page 893 of 1474

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
				3, https://supp ort.apple.com /en- us/HT21260 0, https://supp ort.apple.com /en- us/HT21253 2, https://supp ort.apple.com /en- us/HT21253 3	
Out-of- bounds Write	08-Sep-21	9.3	A malicious application may be able to execute arbitrary code with kernel privileges. This issue is fixed in macOS Big Sur 11.4, Security Update 2021-003 Catalina, Security Update 2021-004 Mojave. An out-of-bounds write issue was addressed with improved bounds checking. CVE ID : CVE-2021-30735	https://supp ort.apple.com /en- us/HT21253 0, https://supp ort.apple.com /en- us/HT21253 1, https://supp ort.apple.com /en- us/HT21252 9	O-APP-MAC 200921/2227
Out-of- bounds Write	08-Sep-21	6.8	A memory corruption issue in the ASN.1 decoder was addressed by removing the vulnerable code. This issue is fixed in tvOS 14.6, Security Update 2021-004 Mojave, iOS 14.6 and iPadOS 14.6, iOS 12.5.4, Security Update 2021- 003 Catalina, macOS Big Sur	https://supp ort.apple.com /en- us/HT21253 0, https://supp ort.apple.com /en- us/HT21253	O-APP-MAC 200921/2228

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			11.4, watchOS 7.5. Processing a maliciously crafted certificate may lead to arbitrary code execution. CVE ID : CVE-2021-30737	1, https://supp ort.apple.com /en- us/HT21252 9, https://supp ort.apple.com /en- us/HT21252 8, https://supp ort.apple.com /en- us/HT21254 8, https://supp ort.apple.com /en- us/HT21253 2	
N/A	08-Sep-21	2.1	A malicious application may be able to overwrite arbitrary files. This issue is fixed in macOS Big Sur 11.4, Security Update 2021-004 Mojave. An issue with path validation logic for hardlinks was addressed with improved path sanitization. CVE ID : CVE-2021-30738	https://supp ort.apple.com /en- us/HT21253 1, https://supp ort.apple.com /en- us/HT21252 9	O-APP-MAC 200921/2229
Out-of- bounds Write	08-Sep-21	4.6	A local attacker may be able to elevate their privileges. This issue is fixed in macOS Big Sur 11.4, Security Update 2021-003 Catalina, Security Update 2021-004 Mojave. A memory corruption issue was addressed with	https://supp ort.apple.com /en- us/HT21253 0, https://supp ort.apple.com /en-	O-APP-MAC 200921/2230

CVSS Scoring Scale

0-1

1-2

7-8

5-6

6-7

8-9

9-10

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			improved validation. CVE ID : CVE-2021-30739	us/HT21253 1, https://supp ort.apple.com /en- us/HT21252 9	
Out-of- bounds Write	08-Sep-21	6.8	An out-of-bounds write was addressed with improved input validation. This issue is fixed in iOS 14.5 and iPadOS 14.5, watchOS 7.4, Security Update 2021-003 Catalina, tvOS 14.5, macOS Big Sur 11.3. Processing a maliciously crafted image may lead to arbitrary code execution. CVE ID : CVE-2021-30743	https://supp ort.apple.com /en- us/HT21253 0, https://supp ort.apple.com /en- us/HT21231 7, https://supp ort.apple.com /en- us/HT21232 5, https://supp ort.apple.com /en- us/HT21232 3, https://supp ort.apple.com /en- us/HT21232 4	O-APP-MAC 200921/2231
Out-of- bounds Write CVSS Scoring So	08-Sep-21	6.8	A stack overflow was addressed with improved input validation. This issue is fixed in iOS 14.7, macOS Big Sur 11.5, watchOS 7.6, tvOS 14.7, Security Update 2021- 005 Mojave, Security Update 2021-004 Catalina.	https://supp ort.apple.com /en- us/HT21260 4, https://supp ort.apple.com /en-	O-APP-MAC 200921/2232 8-9 9-10

Page 896 of 1474

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Processing a maliciously crafted font file may lead to arbitrary code execution. CVE ID : CVE-2021-30759	us/HT21260 5, https://supp ort.apple.com /en- us/HT21260 2, https://supp ort.apple.com /en- us/HT21260 3, https://supp ort.apple.com /en- us/HT21260 0, https://supp ort.apple.com /en- us/HT21260 1	
tvos Improper Authenticati on	08-Sep-21	5.8	A logic issue was addressed with improved restrictions. This issue is fixed in tvOS 14.6, iOS 14.6 and iPadOS 14.6, Safari 14.1.1, macOS Big Sur 11.4, watchOS 7.5. A malicious website may be able to access restricted ports on arbitrary servers. CVE ID : CVE-2021-30720	https://supp ort.apple.com /en- us/HT21252 9, https://supp ort.apple.com /en- us/HT21252 8, https://supp ort.apple.com /en- us/HT21253 4, https://supp ort.apple.com	0-APP-TVOS- 200921/2233

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
				/en- us/HT21253 2, https://supp ort.apple.com /en- us/HT21253 3 https://supp	
N/A	08-Sep-21	4.3	A logic issue was addressed with improved state management. This issue is fixed in macOS Big Sur 11.4, tvOS 14.6, watchOS 7.5, iOS 14.6 and iPadOS 14.6. A malicious application may be able to modify protected parts of the file system. CVE ID : CVE-2021-30727	ort.apple.com /en- us/HT21252 9, https://supp ort.apple.com /en- us/HT21252 8, https://supp ort.apple.com /en- us/HT21253 2, https://supp ort.apple.com /en- us/HT21253 3	0-APP-TVOS- 200921/2234
Out-of- bounds Read CVSS Scoring Sc	08-Sep-21	4.3	An out-of-bounds read was addressed with improved input validation. This issue is fixed in tvOS 14.6, iOS 14.6 and iPadOS 14.6, Security Update 2021-004 Catalina, Security Update 2021-005 Mojave, macOS Big Sur 11.4, watchOS 7.5. Processing a maliciously crafted font may result in the disclosure of	https://supp ort.apple.com /en- us/HT21252 9, https://supp ort.apple.com /en- us/HT21252 8, https://supp ort.apple.com	0-APP-TVOS- 200921/2235

Out-of- bounds08-Sep-216.8Multiple memory corruption infinistave in fixed in type range content in type result in type re	Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Out-of- bounds08-Sep-216.8Multiple memory corruption issues were addressed with improved memory handling. This issue is fixed in tvOS 14.6, iOS 14.6 and iPadOS Sur 11.4, watchOS 7.5.0-APP-TVOS- 200921/2236Out-of- bounds08-Sep-216.814.6, Safari 14.1.1, macOS Big Sur 11.4, watchOS 7.5. Processing maliciously crafted web content may lead to arbitrary code execution. CVE ID : CVE-2021-307340-APP-TVOS- 200921/2236Out-of- bounds0.40014.6Out-of- bounds14.614.6Out-of- bounds14.614.6Out-of- bounds14.614.6Out-of- bounds14.614.6Out-of- bounds14.614.6Out-of- bounds14.614.6Out-of- bounds14.6 <td></td> <td></td> <td></td> <td></td> <td>us/HT21260 3, https://supp ort.apple.com /en- us/HT21260 0, https://supp ort.apple.com /en- us/HT21253 2, https://supp ort.apple.com /en- us/HT21253</td> <td></td>					us/HT21260 3, https://supp ort.apple.com /en- us/HT21260 0, https://supp ort.apple.com /en- us/HT21253 2, https://supp ort.apple.com /en- us/HT21253	
	bounds	08-Sep-21	6.8	issues were addressed with improved memory handling. This issue is fixed in tvOS 14.6, iOS 14.6 and iPadOS 14.6, Safari 14.1.1, macOS Big Sur 11.4, watchOS 7.5. Processing maliciously crafted web content may lead to arbitrary code execution.	ort.apple.com /en- us/HT21252 9, https://supp ort.apple.com /en- us/HT21252 8, https://supp ort.apple.com /en- us/HT21253 4, https://supp ort.apple.com /en- us/HT21253 2, https://supp	

Page 899 of 1474

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
				/en- us/HT21253 3	
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	08-Sep-21	9.3	A buffer overflow was addressed with improved size validation. This issue is fixed in macOS Big Sur 11.4, tvOS 14.6, watchOS 7.5, iOS 14.6 and iPadOS 14.6. An application may be able to execute arbitrary code with kernel privileges. CVE ID : CVE-2021-30736	https://supp ort.apple.com /en- us/HT21252 9, https://supp ort.apple.com /en- us/HT21252 8, https://supp ort.apple.com /en- us/HT21253 2, https://supp ort.apple.com /en- us/HT21253 3	O-APP-TVOS- 200921/2237
Out-of- bounds Write	08-Sep-21	6.8	A memory corruption issue in the ASN.1 decoder was addressed by removing the vulnerable code. This issue is fixed in tvOS 14.6, Security Update 2021-004 Mojave, iOS 14.6 and iPadOS 14.6, iOS 12.5.4, Security Update 2021- 003 Catalina, macOS Big Sur 11.4, watchOS 7.5. Processing a maliciously crafted certificate may lead to arbitrary code execution. CVE ID : CVE-2021-30737	https://supp ort.apple.com /en- us/HT21253 0, https://supp ort.apple.com /en- us/HT21253 1, https://supp ort.apple.com /en- us/HT21252 9, https://supp ort.apple.com	O-APP-TVOS- 200921/2238

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
				/en- us/HT21252 8, https://supp ort.apple.com /en- us/HT21254 8, https://supp ort.apple.com /en- us/HT21253 2	
N/A	08-Sep-21	9.3	A logic issue was addressed with improved validation. This issue is fixed in macOS Big Sur 11.4, tvOS 14.6, watchOS 7.5, iOS 14.6 and iPadOS 14.6. A malicious application may be able to execute arbitrary code with kernel privileges. CVE ID : CVE-2021-30740	https://supp ort.apple.com /en- us/HT21252 9, https://supp ort.apple.com /en- us/HT21252 8, https://supp ort.apple.com /en- us/HT21253 2, https://supp ort.apple.com /en- us/HT21253 3	0-APP-TVOS- 200921/2239
Out-of- bounds Write CVSS Scoring Sc	08-Sep-21	6.8	An out-of-bounds write was addressed with improved input validation. This issue is fixed in iOS 14.5 and iPadOS 14.5, watchOS 7.4, Security Update 2021-003 Catalina, tvOS 14.5, macOS Big Sur	https://supp ort.apple.com /en- us/HT21253 0, https://supp ort.apple.com	0-APP-TVOS- 200921/2240 8-9 9-10

Access of Resource Using Incompatible Confusion')08-Sep-216.8A type confusion issue was addressed with improved state handling. This issue is fixed in 105 14.7, Starpi 14.1.2, macOS Big Sur 11.5, watchOS 7.6, tvOS 14.7. Processing maliciously crafted web content may lead to arbitrary code executionAPP-TVOS- 200921/2241 (en- us/HT212260 5, https://supp ort.apple.com /en- us/HT21232 3, https://supp ort.apple.com /en- us/HT21232 4Access of Resource Using Incompatible (Type Confusion')08-Sep-216.8A type confusion issue was addressed with improved state handling. This issue is fixed in 10S 14.7, Safari 14.1.2, macOS Big Sur 11.5, watchOS 7.6, tvOS 14.7. Processing maliciously crafted web content may lead to arbitrary code execution.0-APP-TVOS- 200921/2241 (en- us/HT21260 5, (en- us/HT21260 2, https://supp ort.apple.com /en- us/HT21260 2, https://supp ort.apple.com /en- us/HT21260 2, https://supp ort.apple.com /en- us/HT21260 2, https://supp ort.apple.com /en- us/HT21260 2, https://supp ort.apple.com /en- us/HT21260 2, https://supp ort.apple.com /en- us/HT21260 2, https://supp ort.apple.com	Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Access of Resource Using Incompatible Confusion's08-Sep-216.8A type confusion issue was addressed with improved state handling. This issue is fixed in iOS 14.7, Safari 14.1.2, macOS Big Sur 11.5, watchOS 7.6, tvOS 14.7. Processing maliciously crafted web content may lead to arbitrary code execution.ortapple.com (en- us/HT21260) 4, https://supp ortapple.com /en- us/HT21260 5, crafted web content may lead to arbitrary code execution.O-APP-TVOS- 200921/2241CVF ID : CVE-2021-30758https://supp ortapple.com /en- us/HT21260 5, ortapple.com /en- us/HT21260 2, https://suppO-APP-TUOS- 200921/2241				maliciously crafted image may lead to arbitrary code execution.	us/HT21231 7, https://supp ort.apple.com /en- us/HT21232 5, https://supp ort.apple.com /en- us/HT21232 3, https://supp ort.apple.com /en- us/HT21232	
	Resource Using Incompatibl e Type ('Type	08-Sep-21	6.8	addressed with improved state handling. This issue is fixed in iOS 14.7, Safari 14.1.2, macOS Big Sur 11.5, watchOS 7.6, tvOS 14.7. Processing maliciously crafted web content may lead to arbitrary code execution.	ort.apple.com /en- us/HT21260 6, https://supp ort.apple.com /en- us/HT21260 4, https://supp ort.apple.com /en- us/HT21260 5, https://supp ort.apple.com /en- us/HT21260 2, https://supp	

3-4 4-5 Page 902 of 1474

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
				/en- us/HT21260 1	
Out-of- bounds Write	08-Sep-21	6.8	A stack overflow was addressed with improved input validation. This issue is fixed in iOS 14.7, macOS Big Sur 11.5, watchOS 7.6, tvOS 14.7, Security Update 2021- 005 Mojave, Security Update 2021-004 Catalina. Processing a maliciously crafted font file may lead to arbitrary code execution. CVE ID : CVE-2021-30759	https://supp ort.apple.com /en- us/HT21260 4, https://supp ort.apple.com /en- us/HT21260 5, https://supp ort.apple.com /en- us/HT21260 2, https://supp ort.apple.com /en- us/HT21260 3, https://supp ort.apple.com /en- us/HT21260 0, https://supp ort.apple.com /en- us/HT21260 1	O-APP-TVOS- 200921/2242
N/A	08-Sep-21	6.8	Processing a maliciously crafted file may lead to arbitrary code execution. This issue is fixed in iOS 14.5 and iPadOS 14.5, watchOS 7.4, tvOS 14.5. This issue was addressed with improved	https://supp ort.apple.com /en- us/HT21231 7, https://supp ort.apple.com	O-APP-TVOS- 200921/2243
CVSS Scoring So	cale 0-1	1-2	2-3 3-4 4-5 5-6	6-7 7-8	8-9 9-10

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			checks. CVE ID : CVE-2021-30764	/en- us/HT21232 3, https://supp ort.apple.com /en- us/HT21232 4	
N/A	08-Sep-21	6.8	This issue was addressed with improved checks. This issue is fixed in iOS 14.7, Safari 14.1.2, macOS Big Sur 11.5, watchOS 7.6, tvOS 14.7. Processing maliciously crafted web content may lead to code execution. CVE ID : CVE-2021-30797	https://supp ort.apple.com /en- us/HT21260 6, https://supp ort.apple.com /en- us/HT21260 4, https://supp ort.apple.com /en- us/HT21260 5, https://supp ort.apple.com /en- us/HT21260 2, https://supp ort.apple.com /en- us/HT21260 1	O-APP-TVOS- 200921/2244
watchos					
Improper Authenticati on	08-Sep-21	5.8	A logic issue was addressed with improved restrictions. This issue is fixed in tvOS 14.6, iOS 14.6 and iPadOS 14.6, Safari 14.1.1, macOS Big	https://supp ort.apple.com /en- us/HT21252 9,	O-APP-WATC- 200921/2245

CVSS Scoring Scale	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10
			P	age 904 c	of 1474					

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Sur 11.4, watchOS 7.5. A malicious website may be able to access restricted ports on arbitrary servers.	https://supp ort.apple.com /en- us/HT21252	
			CVE ID : CVE-2021-30720	8, https://supp ort.apple.com /en- us/HT21253 4, https://supp ort.apple.com /en- us/HT21253 2, https://supp ort.apple.com /en- us/HT21253 3	
Improper Privilege Managemen t	08-Sep-21	4.6	This issue was addressed with improved checks. This issue is fixed in tvOS 14.6, Security Update 2021-004 Mojave, iOS 14.6 and iPadOS 14.6, Security Update 2021- 003 Catalina, macOS Big Sur 11.4, watchOS 7.5. A local attacker may be able to elevate their privileges. CVE ID : CVE-2021-30724	https://supp ort.apple.com /en- us/HT21253 0, https://supp ort.apple.com /en- us/HT21253 1, https://supp ort.apple.com /en- us/HT21252 9, https://supp ort.apple.com /en- us/HT21252 8,	O-APP-WATC- 200921/2246

3-4 4-5 Page 905 of 1474

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
				https://supp ort.apple.com /en- us/HT21253 2, https://supp ort.apple.com /en- us/HT21253 3	
N/A	08-Sep-21	4.3	A logic issue was addressed with improved state management. This issue is fixed in macOS Big Sur 11.4, tvOS 14.6, watchOS 7.5, iOS 14.6 and iPadOS 14.6. A malicious application may be able to modify protected parts of the file system. CVE ID : CVE-2021-30727	https://supp ort.apple.com /en- us/HT21252 9, https://supp ort.apple.com /en- us/HT21252 8, https://supp ort.apple.com /en- us/HT21253 2, https://supp ort.apple.com /en- us/HT21253 3	O-APP-WATC- 200921/2247
Out-of- bounds Read CVSS Scoring Sc	08-Sep-21	4.3	An out-of-bounds read was addressed with improved input validation. This issue is fixed in tvOS 14.6, iOS 14.6 and iPadOS 14.6, Security Update 2021-004 Catalina, Security Update 2021-005 Mojave, macOS Big Sur 11.4, watchOS 7.5. Processing a maliciously crafted font may	https://supp ort.apple.com /en- us/HT21252 9, https://supp ort.apple.com /en- us/HT21252 8, 6-7 7-8	0-APP-WATC- 200921/2248 8-9 9-10

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			result in the disclosure of process memory. CVE ID : CVE-2021-30733	https://supp ort.apple.com /en- us/HT21260 3, https://supp ort.apple.com /en- us/HT21260 0, https://supp ort.apple.com /en- us/HT21253 2, https://supp ort.apple.com /en- us/HT21253 3	
Out-of- bounds Write	08-Sep-21	6.8	Multiple memory corruption issues were addressed with improved memory handling. This issue is fixed in tvOS 14.6, iOS 14.6 and iPadOS 14.6, Safari 14.1.1, macOS Big Sur 11.4, watchOS 7.5. Processing maliciously crafted web content may lead to arbitrary code execution. CVE ID : CVE-2021-30734	https://supp ort.apple.com /en- us/HT21252 9, https://supp ort.apple.com /en- us/HT21252 8, https://supp ort.apple.com /en- us/HT21253 4, https://supp ort.apple.com /en- us/HT21253 2,	O-APP-WATC- 200921/2249

Page 907 of 1474

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
				https://supp ort.apple.com /en- us/HT21253 3	
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	08-Sep-21	9.3	A buffer overflow was addressed with improved size validation. This issue is fixed in macOS Big Sur 11.4, tvOS 14.6, watchOS 7.5, iOS 14.6 and iPadOS 14.6. An application may be able to execute arbitrary code with kernel privileges. CVE ID : CVE-2021-30736	https://supp ort.apple.com /en- us/HT21252 9, https://supp ort.apple.com /en- us/HT21252 8, https://supp ort.apple.com /en- us/HT21253 2, https://supp ort.apple.com /en- us/HT21253 3	O-APP-WATC- 200921/2250
Out-of- bounds Write	08-Sep-21	6.8	A memory corruption issue in the ASN.1 decoder was addressed by removing the vulnerable code. This issue is fixed in tvOS 14.6, Security Update 2021-004 Mojave, iOS 14.6 and iPadOS 14.6, iOS 12.5.4, Security Update 2021- 003 Catalina, macOS Big Sur 11.4, watchOS 7.5. Processing a maliciously crafted certificate may lead to arbitrary code execution. CVE ID : CVE-2021-30737	https://supp ort.apple.com /en- us/HT21253 0, https://supp ort.apple.com /en- us/HT21253 1, https://supp ort.apple.com /en- us/HT21252 9,	O-APP-WATC- 200921/2251

Page 908 of 1474

			Description & CVE ID		NCIIPC ID
				https://supp ort.apple.com /en- us/HT21252 8, https://supp ort.apple.com /en- us/HT21254 8, https://supp ort.apple.com /en- us/HT21253 2	
N/A	08-Sep-21	9.3	A logic issue was addressed with improved validation. This issue is fixed in macOS Big Sur 11.4, tvOS 14.6, watchOS 7.5, iOS 14.6 and iPadOS 14.6. A malicious application may be able to execute arbitrary code with kernel privileges. CVE ID : CVE-2021-30740	https://supp ort.apple.com /en- us/HT21252 9, https://supp ort.apple.com /en- us/HT21252 8, https://supp ort.apple.com /en- us/HT21253 2, https://supp ort.apple.com /en- us/HT21253 3	O-APP-WATC- 200921/2252
Out-of- bounds Write	08-Sep-21	6.8	An out-of-bounds write was addressed with improved input validation. This issue is fixed in iOS 14.5 and iPadOS 14.5, watchOS 7.4, Security	https://supp ort.apple.com /en- us/HT21253 0,	0-APP-WATC- 200921/2253

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Update 2021-003 Catalina, tvOS 14.5, macOS Big Sur 11.3. Processing a maliciously crafted image may lead to arbitrary code execution. CVE ID : CVE-2021-30743	https://supp ort.apple.com /en- us/HT21231 7, https://supp ort.apple.com /en- us/HT21232 5, https://supp ort.apple.com /en- us/HT21232 3, https://supp ort.apple.com /en- us/HT21232 4	
Access of Resource Using Incompatibl e Type ('Type Confusion')	08-Sep-21	6.8	A type confusion issue was addressed with improved state handling. This issue is fixed in iOS 14.7, Safari 14.1.2, macOS Big Sur 11.5, watchOS 7.6, tvOS 14.7. Processing maliciously crafted web content may lead to arbitrary code execution. CVE ID : CVE-2021-30758	https://supp ort.apple.com /en- us/HT21260 6, https://supp ort.apple.com /en- us/HT21260 4, https://supp ort.apple.com /en- us/HT21260 5, https://supp ort.apple.com /en- us/HT21260 2,	O-APP-WATC- 200921/2254

 3-4
 4-5

 Page 910 of 1474

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
				https://supp ort.apple.com /en- us/HT21260 1	
Out-of- bounds Write	08-Sep-21	6.8	A stack overflow was addressed with improved input validation. This issue is fixed in iOS 14.7, macOS Big Sur 11.5, watchOS 7.6, tvOS 14.7, Security Update 2021- 005 Mojave, Security Update 2021-004 Catalina. Processing a maliciously crafted font file may lead to arbitrary code execution. CVE ID : CVE-2021-30759	https://supp ort.apple.com /en- us/HT21260 4, https://supp ort.apple.com /en- us/HT21260 5, https://supp ort.apple.com /en- us/HT21260 2, https://supp ort.apple.com /en- us/HT21260 3, https://supp ort.apple.com /en- us/HT21260 0, https://supp ort.apple.com /en- us/HT21260 1	O-APP-WATC- 200921/2255
Improper Input Validation	08-Sep-21	4.3	An input validation issue was addressed with improved input validation. This issue is fixed in iOS 14.7, watchOS 7.6. A shortcut may be able to	https://supp ort.apple.com /en- us/HT21260 5,	O-APP-WATC- 200921/2256
CVSS Scoring Sc	ale 0-1	1-2	2-3 3-4 4-5 5-6	6-7 7-8	8-9 9-10

N/A08-Sep-216.8bypass Internet permission requirements. CVE ID : CVE-2021-30763https://supp ort.apple.com (en- us/HT21260 1https://supp ort.apple.com (en- us/HT21231 7, https://supp ort.apple.com /en- us/HT21232 3, https://suppotherapie.com ort.apple.com (en- us/HT21232 3, https://suppotherapie.com ort.apple.com (en- us/HT21232 3, https://suppotherapie.com ort.apple.com (en- us/HT21232 4otherapie.com ort.apple.com (en- us/HT21232 4otherapie.com ort.apple.com (en- us/HT21232 4otherapie.com (en- us/HT21232 4otherapie.com (en- us/HT21232 4otherapie.com (en- us/HT21232 4otherapie.com (en- us/HT21232 4otherapie.com (en- us/HT21232 4otherapie.com (en- us/HT21232 4otherapie.com (en- us/HT21232 4otherapie.com (en- us/HT21230 5, https://supp ort.apple.com (en- us/HT21260 5, https://supp ort.apple.com (en- us/HT21260 5, https://supp ort.apple.com (en- us/HT21260 5, https://supp ort.apple.com (en- us/HT21260 5, https://supp ort.apple.com (en- us/HT21260 5, https://supp ort.apple.com (en- us/HT21260 5, https://supp ort.apple.com (en- us/HT21260 5, https://supp ort.apple.com (en- us/HT21260 5, https://supp ort.apple.com (en- us/HT21260 5, https://supp ort.apple.com (en- us/HT21260 5, https://suppotherapie.com (en- us/HT21260 5, https://supp ort.apple.com (en- us/HT21260 5, https://suppotherapie.com (en- us/HT21260 5, https://supp <th>Weakness</th> <th>Publish Date</th> <th>CVSS</th> <th>Description & CVE ID</th> <th>Patch</th> <th>NCIIPC ID</th>	Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
N/A 08-Sep-21 4.8 A A A A A A A A A A A A A A A A A A A				requirements.	ort.apple.com /en- us/HT21260	
N/A 08-Sep-21 6.8 6.8 First issue was addressed 0.4 memory 0.4 mem	N/A	08-Sep-21	6.8	crafted file may lead to arbitrary code execution. This issue is fixed in iOS 14.5 and iPadOS 14.5, watchOS 7.4, tvOS 14.5. This issue was addressed with improved checks.	ort.apple.com /en- us/HT21231 7, https://supp ort.apple.com /en- us/HT21232 3, https://supp ort.apple.com /en- us/HT21232 4	
	N/A	08-Sep-21	6.8	with improved checks. This issue is fixed in iOS 14.7, Safari 14.1.2, macOS Big Sur 11.5, watchOS 7.6, tvOS 14.7. Processing maliciously crafted web content may lead to code execution.	ort.apple.com /en- us/HT21260 6, https://supp ort.apple.com /en- us/HT21260 4, https://supp ort.apple.com /en- us/HT21260 5, https://supp ort.apple.com /en-	

Page 912 of 1474

Weakness	Publish Date	CVSS	Description & CVE ID		Patch	NCIIPC ID
					https://supp ort.apple.com /en- us/HT21260 1	
Exposure of Resource to Wrong Sphere	08-Sep-21	7.8	A logic issue was addres with improved state management. This issue fixed in iOS 14.7, macOS Sur 11.5, watchOS 7.6. A malicious application ma able to bypass certain Privacy preferences. CVE ID : CVE-2021-307	is Big ay be	https://supp ort.apple.com /en- us/HT21260 5, https://supp ort.apple.com /en- us/HT21260 2, https://supp ort.apple.com /en- us/HT21260 1	0-APP-WATC- 200921/2259
Arubanetwo arubaos	rks					
Improper Neutralizati on of Special Elements used in a Command ('Command Injection')	07-Sep-21	9	A remote arbitrary commexecution vulnerability of discovered in Aruba SD-Software and Gateways; Aruba Operating System Software version(s): Price 8.6.0.4-2.2.0.4; Prior to 8.7.1.4, 8.6.0.9, 8.5.0.13, 8.3.0.16, 6.5.4.20, 6.4.4.2 Aruba has released patch for Aruba SD-WAN Software discovered and Gateways and Aruba that address this security vulnerability. CVE ID : CVE-2021-377	was WAN or to 25. hes vare aOS y	https://www. arubanetwor ks.com/asset s/alert/ARUB A-PSA-2021- 016.txt	O-ARU-ARUB- 200921/2260
Improper	07-Sep-21	9	A remote arbitrary com	mand	https://www.	O-ARU-ARUB-
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 & CVE ID	Patch	NCIIPC ID
Neutralizati on of Special Elements used in a Command ('Command Injection')			execution vulnerability was discovered in Aruba Operating System Software version(s): Prior to 8.7.1.2, 8.6.0.8, 8.5.0.12, 8.3.0.16. Aruba has released patches for ArubaOS that address this security vulnerability. CVE ID : CVE-2021-37723	arubanetwor ks.com/asset s/alert/ARUB A-PSA-2021- 016.txt	200921/2261
Improper Neutralizati on of Special Elements used in a Command ('Command Injection')	07-Sep-21	9	A remote arbitrary command execution vulnerability was discovered in Aruba Operating System Software version(s): Prior to 8.7.1.2, 8.6.0.8, 8.5.0.12, 8.3.0.16. Aruba has released patches for ArubaOS that address this security vulnerability. CVE ID : CVE-2021-37724	https://www. arubanetwor ks.com/asset s/alert/ARUB A-PSA-2021- 016.txt	O-ARU-ARUB- 200921/2262
Cross-Site Request Forgery (CSRF)	07-Sep-21	5.8	A remote cross-site request forgery (csrf) vulnerability was discovered in Aruba SD- WAN Software and Gateways; Aruba Operating System Software version(s): Prior to 8.6.0.4-2.2.0.4; Prior to 8.8.0.1, 8.7.1.2, 8.6.0.8, 8.5.0.12, 8.3.0.15. Aruba has released patches for Aruba SD-WAN Software and Gateways and ArubaOS that address this security vulnerability. CVE ID : CVE-2021-37725	https://www. arubanetwor ks.com/asset s/alert/ARUB A-PSA-2021- 016.txt	O-ARU-ARUB- 200921/2263
Improper Limitation of a Pathname to	07-Sep-21	5.5	A remote path traversal vulnerability was discovered in Aruba Operating System Software version(s): Prior to	https://www. arubanetwor ks.com/asset s/alert/ARUB	O-ARU-ARUB- 200921/2264

CVSS Scoring Scale	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10
			D	0110	£1474					

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
a Restricted Directory ('Path Traversal')			8.8.0.1, 8.7.1.4, 8.6.0.11, 8.5.0.13. Aruba has released patches for ArubaOS that address this security vulnerability. CVE ID : CVE-2021-37728	A-PSA-2021- 016.txt	
Improper Limitation of a Pathname to a Restricted Directory ('Path Traversal')	07-Sep-21	5.5	A remote path traversal vulnerability was discovered in Aruba SD-WAN Software and Gateways; Aruba Operating System Software version(s): Prior to 8.6.0.0- 2.2.0.4; Prior to 8.7.1.3, 8.6.0.9, 8.5.0.12, 8.3.0.16, 6.5.4.19, 6.4.4.25. Aruba has released patches for Aruba SD-WAN Software and Gateways and ArubaOS that address this security vulnerability. CVE ID : CVE-2021-37729	https://www. arubanetwor ks.com/asset s/alert/ARUB A-PSA-2021- 016.txt	O-ARU-ARUB- 200921/2265
Improper Limitation of a Pathname to a Restricted Directory ('Path Traversal')	07-Sep-21	7.2	A local path traversal vulnerability was discovered in Aruba SD-WAN Software and Gateways; Aruba Operating System Software version(s): Prior to 8.6.0.0- 2.2.0.4; Prior to 8.7.1.1, 8.6.0.7, 8.5.0.12, 8.3.0.16. Aruba has released patches for Aruba SD-WAN Software and Gateways and ArubaOS that address this security vulnerability. CVE ID : CVE-2021-37731	https://www. arubanetwor ks.com/asset s/alert/ARUB A-PSA-2021- 016.txt	O-ARU-ARUB- 200921/2266
Improper Limitation of a	07-Sep-21	4	A remote path traversal vulnerability was discovered in Aruba SD-WAN Software	https://www. arubanetwor ks.com/asset	O-ARU-ARUB- 200921/2267

CVSS Scoring Scale	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10	
Page 915 of 1/17/											

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Pathname to a Restricted Directory ('Path Traversal')		Operating System Software version(s): Prior to 8.6.0.4- 2.2.0.4; Prior to 8.7.1.1, 8.6.0.7, 8.5.0.11, 8.3.0.16. Aruba has released patches for Aruba SD-WAN Software and Gateways and ArubaOS that address this security vulnerability. CVE ID : CVE-2021-37733		s/alert/ARUB A-PSA-2021- 016.txt	
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	07-Sep-21	7.5	A remote buffer overflow vulnerability was discovered in Aruba SD-WAN Software and Gateways; Aruba Operating System Software version(s): Prior to 8.6.0.4- 2.2.0.4; Prior to 8.7.1.2, 8.6.0.8, 8.5.0.12, 8.3.0.15. Aruba has released patches for Aruba SD-WAN Software and Gateways and ArubaOS that address this security vulnerability. CVE ID : CVE-2021-37716	https://www. arubanetwor ks.com/asset s/alert/ARUB A-PSA-2021- 016.txt	O-ARU-ARUB- 200921/2268
Improper Neutralizati on of Special Elements used in a Command ('Command Injection')	proper utralizati of Special ements ed in a mmand ommand A remote arbitrary command execution vulnerability was discovered in Aruba SD-WAN Software and Gateways; Aruba Operating System Software version(s): Prior to 8.6.0.4-2.2.0.6; Prior to 8.7.1.4, 8.6.0.7, 8.5.0.12, 8.3.0.16. Aruba has released patches for Aruba SD-WAN		https://www. arubanetwor ks.com/asset s/alert/ARUB A-PSA-2021- 016.txt	O-ARU-ARUB- 200921/2269	

CVSS Scoring Scale	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10
			n	010 -	£ 4 4 7 4					

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2021-37717		
Improper Neutralizati on of Special Elements used in a Command ('Command Injection')	ralizati Special eents in a mand nmand		A remote arbitrary command execution vulnerability was discovered in Aruba SD-WAN Software and Gateways; Aruba Operating System Software version(s): Prior to 8.6.0.4-2.2.0.6; Prior to 8.7.1.4, 8.6.0.7, 8.5.0.12, 8.3.0.16. Aruba has released patches for Aruba SD-WAN Software and Gateways and ArubaOS that address this security vulnerability. CVE ID : CVE-2021-37718	https://www. arubanetwor ks.com/asset s/alert/ARUB A-PSA-2021- 016.txt	0-ARU-ARUB- 200921/2270
Improper Neutralizati on of Special Elements used in a Command ('Command Injection')	07-Sep-21	9	A remote arbitrary command execution vulnerability was discovered in Aruba SD-WAN Software and Gateways; Aruba Operating System Software version(s): Prior to 8.6.0.4-2.2.0.4; Prior to 8.7.1.4, 8.6.0.9, 8.5.0.13, 8.3.0.16, 6.5.4.20, 6.4.4.25. Aruba has released patches for Aruba SD-WAN Software and Gateways and ArubaOS that address this security vulnerability. CVE ID : CVE-2021-37719	https://www. arubanetwor ks.com/asset s/alert/ARUB A-PSA-2021- 016.txt	O-ARU-ARUB- 200921/2271
Improper Neutralizati on of Special Elements used in a Command ('Command Injection')	proper eutralizati of Special ements ed in a mmand command		https://www. arubanetwor ks.com/asset s/alert/ARUB A-PSA-2021- 016.txt	0-ARU-ARUB- 200921/2272	

Page 917 of 1474

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Aruba has released patches for Aruba SD-WAN Software and Gateways and ArubaOS that address this security vulnerability. CVE ID : CVE-2021-37720		
Improper Neutralizati on of Special Elements used in a Command ('Command Injection')	07-Sep-21	9	A remote arbitrary command execution vulnerability was discovered in Aruba SD-WAN Software and Gateways; Aruba Operating System Software version(s): Prior to 8.6.0.4-2.2.0.4; Prior to 8.7.1.4, 8.6.0.9, 8.5.0.13, 8.3.0.16, 6.5.4.20, 6.4.4.25. Aruba has released patches for Aruba SD-WAN Software and Gateways and ArubaOS that address this security vulnerability. CVE ID : CVE-2021-37721	https://www. arubanetwor ks.com/asset s/alert/ARUB A-PSA-2021- 016.txt	O-ARU-ARUB- 200921/2273
sd-wan	I			L	L
-		A remote path traversal vulnerability was discovered in Aruba SD-WAN Software and Gateways; Aruba Operating System Software version(s): Prior to 8.6.0.0- 2.2.0.4; Prior to 8.7.1.3, 8.6.0.9, 8.5.0.12, 8.3.0.16, 6.5.4.19, 6.4.4.25. Aruba has released patches for Aruba SD-WAN Software and	https://www. arubanetwor ks.com/asset s/alert/ARUB A-PSA-2021- 016.txt	O-ARU-SD-W- 200921/2274	
('Path Traversal')			Gateways and ArubaOS that address this security vulnerability. CVE ID : CVE-2021-37729		

Page 918 of 1474

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Limitation of a Pathname to a Restricted Directory ('Path Traversal')			vulnerability was discovered in Aruba SD-WAN Software and Gateways; Aruba Operating System Software version(s): Prior to 8.6.0.0- 2.2.0.4; Prior to 8.7.1.1, 8.6.0.7, 8.5.0.12, 8.3.0.16. Aruba has released patches for Aruba SD-WAN Software and Gateways and ArubaOS that address this security vulnerability. CVE ID : CVE-2021-37731	arubanetwor ks.com/asset s/alert/ARUB A-PSA-2021- 016.txt	200921/2275
Improper Limitation of a Pathname to a Restricted Directory ('Path Traversal')	ion me to icted ory 07-Sep-21 4		A remote path traversal vulnerability was discovered in Aruba SD-WAN Software and Gateways; Aruba Operating System Software version(s): Prior to 8.6.0.4- 2.2.0.4; Prior to 8.7.1.1, 8.6.0.7, 8.5.0.11, 8.3.0.16. Aruba has released patches for Aruba SD-WAN Software and Gateways and ArubaOS that address this security vulnerability. CVE ID : CVE-2021-37733	https://www. arubanetwor ks.com/asset s/alert/ARUB A-PSA-2021- 016.txt	O-ARU-SD-W- 200921/2276
bluetrum	uetrum			<u> </u>	
ab5301a_firr	nware				
N/A			The Bluetooth Classic implementation on Bluetrum AB5301A devices with unknown firmware versions does not properly handle the reception of oversized DM1 LMP packets while no other BT connections are active, allowing attackers in radio	http://www. bluetrum.co m/product/a b5301a.html	O-BLU-AB53- 200921/2277

CVSS Scoring Scale	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10
Page 919 of 1474										

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			range to prevent new BT connections (disabling the AB5301A inquiry and page scan procedures) via a crafted LMP packet. The user needs to manually perform a power cycle (restart) of the device to restore BT connectivity.		
ab 527(+ fin			CVE ID : CVE-2021-34150		
ab5376t_firn	iware		The Divete eth Charain		
N/A	07-Sep-21	6.1	The Bluetooth Classic implementation on AB32VG1 devices does not properly handle the reception of continuous unsolicited LMP responses, allowing attackers in radio range to trigger a denial of service (either restart or deadlock the device) by flooding a device with LMP_AU_rand data. CVE ID : CVE-2021-31610	http://www. bluetrum.co m/product/a b5376t.html, http://www. bluetrum.co m/product/b t8896a.html	O-BLU-AB53- 200921/2278
bt8896a_firm	nware				
N/A	07-Sep-21	6.1	The Bluetooth Classic implementation on AB32VG1 devices does not properly handle the reception of continuous unsolicited LMP responses, allowing attackers in radio range to trigger a denial of service (either restart or deadlock the device) by flooding a device with LMP_AU_rand data. CVE ID : CVE-2021-31610	http://www. bluetrum.co m/product/a b5376t.html, http://www. bluetrum.co m/product/b t8896a.html	O-BLU-BT88- 200921/2279
christiedigita	al				

0-1

1-2

6-7

5-6

7-8

8-9

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
dwu850-gs_f	irmware				
Improper Authenticati on	01-Sep-21	7.5	webctrl.cgi.elf on Christie Digital DWU850-GS V06.46 devices allows attackers to perform any desired action via a crafted query containing an unspecified Cookie header. Authentication bypass can be achieved by including an administrative cookie that the device does not validate. CVE ID : CVE-2021-40350	N/A	O-CHR- DWU8- 200921/2280
comprotech					
ip570_firmwa	are				
Missing Authorizatio n	01-Sep-21	8.5	An issue was discovered on Compro IP70 2.08_7130218, IP570 2.08_7130520, IP60, and TN540 devices. /cgi- bin/support/killps.cgi deletes all data from the device. CVE ID : CVE-2021-40378	N/A	O-COM-IP57- 200921/2281
Improper Privilege Managemen t	01-Sep-21	5	An issue was discovered on Compro IP70 2.08_7130218, IP570 2.08_7130520, IP60, and TN540 devices. rstp:///medias2 does not require authorization. CVE ID : CVE-2021-40379	N/A	O-COM-IP57- 200921/2282
Improper Authenticati on	01-Sep-21	5	An issue was discovered on Compro IP70 2.08_7130218, IP570 2.08_7130520, IP60, and TN540 devices. cameralist.cgi and setcamera.cgi disclose credentials.	N/A	O-COM-IP57- 200921/2283
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 & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2021-40380		
Improper Privilege Managemen t	01-Sep-21	5	An issue was discovered on Compro IP70 2.08_7130218, IP570 2.08_7130520, IP60, and TN540 devices. index_MJpeg.cgi allows video access.	N/A	0-COM-IP57- 200921/2284
			CVE ID : CVE-2021-40381		
Improper Privilege Managemen t		5	An issue was discovered on Compro IP70 2.08_7130218, IP570 2.08_7130520, IP60, and TN540 devices. mjpegStreamer.cgi allows video screenshot access.	N/A	O-COM-IP57- 200921/2285
			CVE ID : CVE-2021-40382		
ip60_firmwa	re			1	1
Missing Authorizatio n	01-Sep-21	8.5	An issue was discovered on Compro IP70 2.08_7130218, IP570 2.08_7130520, IP60, and TN540 devices. /cgi- bin/support/killps.cgi deletes all data from the device.	N/A	0-COM-IP60- 200921/2286
			CVE ID : CVE-2021-40378		
Improper Privilege Managemen t	01-Sep-21	5	An issue was discovered on Compro IP70 2.08_7130218, IP570 2.08_7130520, IP60, and TN540 devices. rstp:///medias2 does not require authorization. CVE ID : CVE-2021-40379	N/A	O-COM-IP60- 200921/2287
Improper Authenticati on	01-Sep-21	5	An issue was discovered on Compro IP70 2.08_7130218, IP570 2.08_7130520, IP60, and TN540 devices. cameralist.cgi and setcamera.cgi disclose	N/A	0-COM-IP60- 200921/2288
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 & CVE ID	Patch	NCIIPC ID
			credentials.		
			CVE ID : CVE-2021-40380		
Improper Privilege Managemen t	01-Sep-21	5	An issue was discovered on Compro IP70 2.08_7130218, IP570 2.08_7130520, IP60, and TN540 devices. index_MJpeg.cgi allows video access. CVE ID : CVE-2021-40381	N/A	O-COM-IP60- 200921/2289
Improper Privilege Managemen t	01-Sep-21	5	An issue was discovered on Compro IP70 2.08_7130218, IP570 2.08_7130520, IP60, and TN540 devices. mjpegStreamer.cgi allows video screenshot access. CVE ID : CVE-2021-40382	N/A	O-COM-IP60- 200921/2290
ip70_firmwa	re				
Missing Authorizatio n	01-Sep-21	8.5	An issue was discovered on Compro IP70 2.08_7130218, IP570 2.08_7130520, IP60, and TN540 devices. /cgi- bin/support/killps.cgi deletes all data from the device. CVE ID : CVE-2021-40378	N/A	O-COM-IP70- 200921/2291
Improper Privilege Managemen t	01-Sep-21	5	An issue was discovered on Compro IP70 2.08_7130218, IP570 2.08_7130520, IP60, and TN540 devices. rstp:///medias2 does not require authorization. CVE ID : CVE-2021-40379	N/A	O-COM-IP70- 200921/2292
Improper Authenticati on	01-Sep-21	5	An issue was discovered on Compro IP70 2.08_7130218, IP570 2.08_7130520, IP60, and TN540 devices. cameralist.cgi and	N/A	O-COM-IP70- 200921/2293
CVSS Scoring Sc	ale 0-1	1-2	2-3 3-4 4-5 5-6 Page 923 of 1474	6-7 7-8	8-9 9-10

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			setcamera.cgi disclose credentials.		
			CVE ID : CVE-2021-40380		
Improper Privilege Managemen t	ivilege 01-Sep-21 5		An issue was discovered on Compro IP70 2.08_7130218, IP570 2.08_7130520, IP60, and TN540 devices. index_MJpeg.cgi allows video access. CVE ID : CVE-2021-40381	N/A	O-COM-IP70- 200921/2294
			An issue was discovered on		
Improper Privilege Managemen t	Privilege Managemen 01-Sep-21 5		Compro IP70 2.08_7130218, IP570 2.08_7130520, IP60, and TN540 devices. mjpegStreamer.cgi allows video screenshot access.	N/A	O-COM-IP70- 200921/2295
			CVE ID : CVE-2021-40382		
tn540_firmw	are				
Missing Authorizatio n	01-Sep-21	8.5	An issue was discovered on Compro IP70 2.08_7130218, IP570 2.08_7130520, IP60, and TN540 devices. /cgi- bin/support/killps.cgi deletes all data from the device.	N/A	O-COM-TN54- 200921/2296
			CVE ID : CVE-2021-40378		
Improper Privilege Managemen01-Sep-21Compro IP70 2.08 IP570 2.08_71303 and TN540 device rstp:///medias2		An issue was discovered on Compro IP70 2.08_7130218, IP570 2.08_7130520, IP60, and TN540 devices. rstp:///medias2 does not require authorization.	N/A	O-COM-TN54- 200921/2297	
			CVE ID : CVE-2021-40379		
Improper Authenticati on	01-Sep-21	5	An issue was discovered on Compro IP70 2.08_7130218, IP570 2.08_7130520, IP60, and TN540 devices.	N/A	0-COM-TN54- 200921/2298
CVSS Scoring Sc	ale 0-1	1-2	2-3 3-4 4-5 5-6 Page 924 of 1474	6-7 7-8	8-9 9-10

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			cameralist.cgi and setcamera.cgi disclose credentials.		
			CVE ID : CVE-2021-40380		
Improper Privilege Managemen t	01-Sep-21	5	An issue was discovered on Compro IP70 2.08_7130218, IP570 2.08_7130520, IP60, and TN540 devices. index_MJpeg.cgi allows video access. CVE ID : CVE-2021-40381	N/A	O-COM-TN54- 200921/2299
Improper Privilege Managemen t	01-Sep-21	5	An issue was discovered on Compro IP70 2.08_7130218, IP570 2.08_7130520, IP60, and TN540 devices. mjpegStreamer.cgi allows video screenshot access. CVE ID : CVE-2021-40382	N/A	O-COM-TN54- 200921/2300
Contiki-os					
contiki					
Improper Check for Unusual or Exceptional Conditions	05-Sep-21	5	In Contiki 3.0, Telnet option negotiation is mishandled. During negotiation between a server and a client, the server may fail to give the WILL/WONT or DO/DONT response for DO and WILL commands because of improper handling of exception condition, which leads to property violations and denial of service. Specifically, a server sometimes sends no response, because a fixed buffer space is available for all responses and that space	https://githu b.com/contiki - os/contiki/is sues/2686	O-CON-CONT- 200921/2301

CVSS Scoring Scale	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10
		Page 925 of 1474								

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID				
			may have been exhausted.						
			CVE ID : CVE-2021-40523						
Cypress									
cyw20735b1	_firmware								
N/A	07-Sep-21	6.1	The Bluetooth Classic implementation in the Cypress CYW920735Q60EVB does not properly handle the reception of continuous unsolicited LMP responses, allowing attackers in radio range to trigger a denial of service and restart (crash) of the device by flooding it with LMP_AU_Rand packets after the paging procedure. CVE ID : CVE-2021-34146	https://www. cypress.com/ documentatio n/datasheets /cyw20735b 1-single-chip- bluetooth- transceiver- wireless- input-devices	0-CYP-CYW2- 200921/2302				
cyw920735q	60evb-01_fir	mware	9						
N/A	07-Sep-21	6.1	The Bluetooth Classic implementation in the Cypress CYW920735Q60EVB does not properly handle the reception of continuous unsolicited LMP responses, allowing attackers in radio range to trigger a denial of service and restart (crash) of the device by flooding it with LMP_AU_Rand packets after the paging procedure. CVE ID : CVE-2021-34146	https://www. cypress.com/ documentatio n/datasheets /cyw20735b 1-single-chip- bluetooth- transceiver- wireless- input-devices	0-CYP-CYW9- 200921/2303				
wireless_inte	ernet_connect	civity_f	or_embedded_devices						
N/A	07-Sep-21	2.9	The Bluetooth Classic implementation in the Cypress WICED BT stack through 2.9.0 for CYW20735B1 devices does	https://www. cypress.com/ documentatio n/datasheets /cyw20735b	0-CYP-WIRE- 200921/2304				
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 & CVE ID	Patch	NCIIPC ID
			not properly handle the reception of LMP_max_slot with an invalid Baseband packet type (and LT_ADDRESS and LT_ADDR after completion of the LMF setup procedure, allowing attackers in radio range to trigger a denial of service (firmware crash) via a crafted LMP packet. CVE ID : CVE-2021-34145	· ·	
N/A	07-Sep-21	6.1	The Bluetooth Classic implementation in the Cypress WICED BT stack through 2.9.0 for CYW20735B1 does not properly handle the reception of a malformed LMP timing accuracy response followed by multiple reconnections to the link slave, allowing attacked to exhaust device BT resources and eventually trigger a crash via multiple attempts of sending a crafted LMP timing accuracy response followed by a sudden reconnection with a random BDAddress.	s 1-single-chip- bluetooth- transceiver- wireless- input-devices	0-CYP-WIRE- 200921/2305
N/A	07-Sep-21	6.1	The Bluetooth Classic implementation in the Cypress WICED BT stack through 2.9.0 for CYW20735B1 devices does not properly handle the reception of LMP_max_slot	https://www. cypress.com/ documentatio n/datasheets /cyw20735b 1-single-chip- bluetooth-	0-CYP-WIRE- 200921/2306
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 & CVE ID	Patch	NCIIPC ID
			with a greater ACL Length after completion of the LMP setup procedure, allowing attackers in radio range to trigger a denial of service (firmware crash) via a crafted LMP packet.	transceiver- wireless- input-devices	
			CVE ID : CVE-2021-34148		
Debian					
debian_linux	(
Integer Overflow or Wraparoun d	Integer Overflow or Wraparoun d (08-Sep-21) 5 HAProxy 2.0 through 2. htx_add_header that can exploited to perform an HTTP request smugglin attack, allowing an attack to bypass all configured request HAProxy ACLs a possibly other ACLs.		An integer overflow exists in HAProxy 2.0 through 2.5 in htx_add_header that can be exploited to perform an HTTP request smuggling attack, allowing an attacker to bypass all configured http- request HAProxy ACLs and possibly other ACLs. CVE ID : CVE-2021-40346	https://git.ha proxy.org/?p =haproxy.git, https://githu b.com/hapro xy/haproxy/c ommit/3b69 886f7dcc3cfb 3d16630901 8e6cfec9ce2c 95	O-DEB-DEBI- 200921/2307
Fedoraproje	ct				
fedora					
Out-of- bounds Write	06-Sep-21	4.6	vim is vulnerable to Heap- based Buffer Overflow CVE ID : CVE-2021-3770	https://githu b.com/vim/vi m/commit/b 7081e135a16 091c93f6f5f7 525a5c58fb7 ca9f9, https://huntr .dev/bounties /016ad2f2- 07c1-4d14- a8ce- 6eed1072936 5	O-FED-FEDO- 200921/2308

CVSS Scoring Scale	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10
Page 928 of 1474										

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Google	I	<u> </u>		I	
android					
N/A	02-Sep-21	4	Microsoft Edge for Android Spoofing Vulnerability CVE ID : CVE-2021-38641	https://porta l.msrc.micros oft.com/en- US/security- guidance/adv isory/CVE- 2021-38641	0-GOO-ANDR- 200921/2309
N/A	02-Sep-21	4.3	Microsoft Edge for Android Information Disclosure Vulnerability CVE ID : CVE-2021-26439	https://porta l.msrc.micros oft.com/en- US/security- guidance/adv isory/CVE- 2021-26439	O-GOO-ANDR- 200921/2310
chrome_os					
Use After Free	03-Sep-21	6.8	Use after free in WebRTC in Google Chrome on Linux, ChromeOS prior to 93.0.4577.63 allowed an attacker who convinced a user to install a malicious extension to potentially exploit heap corruption via a crafted HTML page. CVE ID : CVE-2021-30611	https://chro mereleases.g oogleblog.co m/2021/08/ stable- channel- update-for- desktop_31.ht ml	0-GOO-CHRO- 200921/2311
Use After Free	03-Sep-21	6.8	Use after free in WebRTC in Google Chrome on Linux, ChromeOS prior to 93.0.4577.63 allowed an attacker who convinced a user to install a malicious extension to potentially exploit heap corruption via a crafted HTML page. CVE ID : CVE-2021-30612	https://chro mereleases.g oogleblog.co m/2021/08/ stable- channel- update-for- desktop_31.ht ml	0-GOO-CHRO- 200921/2312

CVSS Scoring Scale	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10
Page 020 of 1474										

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID			
jbl	I	<u>.</u>						
tune500bt_f	tune500bt_firmware							
N/A	07-Sep-21	6.1	The Bluetooth Classic implementation on JBL TUNE500BT devices does not properly handle the reception of continuous unsolicited LMP responses, allowing attackers in radio range to trigger a denial of service and shutdown a device by flooding the target device with LMP Feature Response data. CVE ID : CVE-2021-28155	https://www. jbl.com.sg/ov er-ear- headphones/J BL+TUNE500 BT.html	O-JBL-TUNE- 200921/2313			
kpn								
experia_wifi	firmware							
Improper Input Validation	01-Sep-21	9	Wireless devices running certain Arcadyan-derived firmware (such as KPN Experia WiFi 1.00.15) do not properly sanitise user input to the syslog configuration form. An authenticated remote attacker could leverage this to alter the device configuration and achieve remote code execution. This can be exploited in conjunction with CVE-2021-20090. CVE ID : CVE-2021-38703	https://www. kpnwebshop. com/modems - routers/prod ucten/experi a-wifi/2	O-KPN-EXPE- 200921/2314			
Linux								
linux_kernel			A 11.1					
Concurrent Execution using	03-Sep-21	4.4	A race condition was discovered in ext4_write_inline_data_end in	https://git.ke rnel.org/pub /scm/linux/k	O-LIN-LINU- 200921/2315			
CVSS Scoring S	cale 0-1	1-2	2-3 3-4 4-5 5-6	6-7 7-8	8-9 9-10			

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Shared Resource with Improper Synchroniza tion ('Race Condition')			fs/ext4/inline.c in the ext4 subsystem in the Linux kernel through 5.13.13. CVE ID : CVE-2021-40490	ernel/git/tyts o/ext4.git/co mmit/?id=9e 445093e523f 3277081314c 864f708fd4b d34aa	
Use After Free	03-Sep-21	6.8	Use after free in WebRTC in Google Chrome on Linux, ChromeOS prior to 93.0.4577.63 allowed an attacker who convinced a user to install a malicious extension to potentially exploit heap corruption via a crafted HTML page. CVE ID : CVE-2021-30611	https://chro mereleases.g oogleblog.co m/2021/08/ stable- channel- update-for- desktop_31.ht ml	O-LIN-LINU- 200921/2316
Use After Free	03-Sep-21	6.8	Use after free in WebRTC in Google Chrome on Linux, ChromeOS prior to 93.0.4577.63 allowed an attacker who convinced a user to install a malicious extension to potentially exploit heap corruption via a crafted HTML page. CVE ID : CVE-2021-30612	https://chro mereleases.g oogleblog.co m/2021/08/ stable- channel- update-for- desktop_31.ht ml	0-LIN-LINU- 200921/2317
mi					
mi_true_wire	eless_earbuds	_basic	_2_firmware		
N/A	07-Sep-21	6.1	The Bluetooth Classic implementation on AB32VG1 devices does not properly handle the reception of continuous unsolicited LMP responses, allowing attackers in radio range to trigger a denial of service (either restart or deadlock the		O-MI-MI_T- 200921/2318
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 & CVE ID	Patch	NCIIPC ID				
			device) by flooding a device with LMP_AU_rand data.						
			CVE ID : CVE-2021-31610						
Microsoft									
windows									
Improper Restriction of Operations within the Bounds of a Memory Buffer	01-Sep-21	9.3	Adobe Bridge version 11.1 (and earlier) is affected by a memory corruption vulnerability due to insecure handling of a malicious Bridge 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-2021-39816	https://helpx .adobe.com/s ecurity/prod ucts/bridge/ apsb21- 69.html	O-MIC-WIND- 200921/2319				
Improper Restriction of Operations within the Bounds of a Memory Buffer	01-Sep-21	9.3	Adobe Bridge version 11.1 (and earlier) is affected by a memory corruption vulnerability due to insecure handling of a malicious Bridge 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-2021-39817	https://helpx .adobe.com/s ecurity/prod ucts/bridge/ apsb21- 69.html	O-MIC-WIND- 200921/2320				
Out-of- bounds Write	02-Sep-21	6.8	Acrobat Reader DC versions versions 2020.013.20074 (and earlier), 2020.001.30018 (and earlier) and 2017.011.30188 (and earlier) are affected by an Out-of-bounds Write vulnerability in the CoolType library. An unauthenticated	https://helpx .adobe.com/s ecurity/prod ucts/acrobat/ apsb21- 09.html	O-MIC-WIND- 200921/2321				

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			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-2021-21086		
Access of Memory Location After End of Buffer	08-Sep-21	9.3	Adobe Illustrator version 25.2 (and earlier) is affected by a memory corruption vulnerability when parsing a specially crafted file. An unauthenticated attacker could leverage this vulnerability to disclose sensitive memory information 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-2021-21103	https://helpx .adobe.com/s ecurity/prod ucts/illustrat or/apsb21- 24.html	O-MIC-WIND- 200921/2322
Access of Memory Location After End of Buffer	08-Sep-21	9.3	Adobe Illustrator version 25.2 (and earlier) is affected by a memory corruption vulnerability when parsing a specially crafted file. An unauthenticated attacker could leverage this vulnerability to remote 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-2021-21104	https://helpx .adobe.com/s ecurity/prod ucts/illustrat or/apsb21- 24.html	O-MIC-WIND- 200921/2323

CVSS Scoring Scale	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10
Page 933 of 1474										

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Access of Memory Location After End of Buffer	08-Sep-21	9.3	Adobe Illustrator version 25.2 (and earlier) is affected by a memory corruption vulnerability when parsing a specially crafted file. An unauthenticated attacker could leverage this vulnerability to achieve remote 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-2021-21105	https://helpx .adobe.com/s ecurity/prod ucts/illustrat or/apsb21- 24.html	O-MIC-WIND- 200921/2324
Creation of Temporary File in Directory with Insecure Permissions	08-Sep-21	6.9	Adobe Genuine Services version 7.1 (and earlier) is affected by an Insecure file permission vulnerability during installation process. A local authenticated attacker could leverage this vulnerability to achieve privilege escalation in the context of the current user. CVE ID : CVE-2021-28568	https://helpx .adobe.com/s ecurity/prod ucts/integrity _service/apsb 21-27.html	0-MIC-WIND- 200921/2325
Out-of- bounds Read	08-Sep-21	4.3	Adobe Media Encoder version 15.1 (and earlier) is affected by an Out-of-bounds Read vulnerability when parsing a specially crafted file. An unauthenticated attacker could leverage this vulnerability to disclose sensitive memory information in the context of the current user. Exploitation of this issue requires user interaction in that a victim	https://helpx .adobe.com/s ecurity/prod ucts/media- encoder/apsb 21-32.html	0-MIC-WIND- 200921/2326
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 & CVE ID	Patch	NCIIPC ID
			must open a malicious file.		
			CVE ID : CVE-2021-28569		
Improper Neutralizati on of Special Elements used in an OS Command ('OS Command Injection')	08-Sep-21	7.6	Adobe After Effects version 18.1 (and earlier) is affected by a potential Command injection vulnerability when chained with a development and debugging tool for JavaScript scripts. 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-2021-28571	https://helpx .adobe.com/e e/security/pr oducts/after_ effects/apsb2 1-33.html	O-MIC-WIND- 200921/2327
Uncontrolle d Search Path Element	08-Sep-21	4.4	Adobe Creative Cloud Desktop 3.5 (and earlier) is affected by an uncontrolled search path vulnerability that could result in elevation of privileges. Exploitation of this issue requires user interaction in that a victim must log on to the attacker's local machine. CVE ID : CVE-2021-28581	https://helpx .adobe.com/s ecurity/prod ucts/creative - cloud/apsb21 -31.html	O-MIC-WIND- 200921/2328
Loop with Unreachable Exit Condition ('Infinite Loop')	07-Sep-21	4.3	A vulnerability affecting F- Secure Antivirus engine was discovered whereby scanning WIM archive file can lead to denial-of-service (infinite loop and freezes AV engine scanner). The vulnerability can be exploit	https://www. f- secure.com/e n/business/p rograms/vuln erability- reward- program/hall	O-MIC-WIND- 200921/2329

0-1

1-2

6-7

5-6

7-8

8-9

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			remotely by an attacker. A successful attack will result in Denial-of-Service of the Anti-Virus engine. CVE ID : CVE-2021-33599	-of-fame, https://www. f- secure.com/e n/business/s upport-and- downloads/s ecurity- advisories/cv e-2021- 33599	
Out-of- bounds Write	02-Sep-21	9.3	Adobe After Effects version 18.2.1 (and earlier) is affected by an out-of-bounds Write vulnerability when parsing a specially crafted 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-2021-35994	https://helpx .adobe.com/s ecurity/prod ucts/after_eff ects/apsb21- 54.html	O-MIC-WIND- 200921/2330
Improper Input Validation	02-Sep-21	4.3	Adobe After Effects version 18.2.1 (and earlier) is affected by an Improper input validation vulnerability when parsing a specially crafted file. An unauthenticated attacker could leverage this vulnerability to disclose arbitrary memory information in the context of the current user. Exploitation of this issue requires user	https://helpx .adobe.com/s ecurity/prod ucts/after_eff ects/apsb21- 54.html	O-MIC-WIND- 200921/2331

0-1

1-2

5-6

6-7

7-8

8-9

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			interaction in that a victim must open a malicious file. CVE ID : CVE-2021-35995		
Access of Memory Location After End of Buffer	02-Sep-21	9.3	Adobe After Effects version 18.2.1 (and earlier) is affected by a memory corruption vulnerability when parsing a specially crafted 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-2021-35996	https://helpx .adobe.com/s ecurity/prod ucts/after_eff ects/apsb21- 54.html	O-MIC-WIND- 200921/2332
Improper Restriction of Operations within the Bounds of a Memory Buffer	02-Sep-21	9.3	Adobe After Effects version 18.2.1 (and earlier) is affected by a memory corruption vulnerability when parsing a specially crafted 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-2021-36017	https://helpx .adobe.com/s ecurity/prod ucts/after_eff ects/apsb21- 54.html	O-MIC-WIND- 200921/2333
Out-of- bounds Read	02-Sep-21	4.3	Adobe After Effects version 18.2.1 (and earlier) is affected by an Out-of-bounds	https://helpx .adobe.com/s ecurity/prod	O-MIC-WIND- 200921/2334
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 & CVE ID	Patch	NCIIPC ID
			Read vulnerability when parsing a specially crafted file. An unauthenticated attacker could leverage this vulnerability to disclose sensitive memory information 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-2021-36018	ucts/after_eff ects/apsb21- 54.html	
Out-of- bounds Read	02-Sep-21	4.3	Adobe After Effects version 18.2.1 (and earlier) is affected by an Out-of-bounds Read vulnerability when parsing a specially crafted file. An unauthenticated attacker could leverage this vulnerability to disclose arbitrary memory information 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-2021-36019	https://helpx .adobe.com/s ecurity/prod ucts/after_eff ects/apsb21- 54.html	O-MIC-WIND- 200921/2335
Improper Restriction of Operations within the Bounds of a Memory Buffer	01-Sep-21	9.3	Adobe Bridge version 11.1 (and earlier) is affected by a memory corruption vulnerability due to insecure handling of a malicious Bridge file, potentially resulting in arbitrary code execution in the context of the current user. User interaction is required to exploit this vulnerability.	https://helpx .adobe.com/s ecurity/prod ucts/bridge/ apsb21- 69.html	0-MIC-WIND- 200921/2336

CVSS Scoring Scale	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10
Page 938 of 1474										

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2021-36059		
Out-of- bounds Write	01-Sep-21	9.3	Adobe Photoshop versions 21.2.10 (and earlier) and 22.4.3 (and earlier) are affected by a heap-based buffer overflow 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 file. CVE ID : CVE-2021-36065	https://helpx .adobe.com/s ecurity/prod ucts/photosh op/apsb21- 68.html	O-MIC-WIND- 200921/2337
Out-of- bounds Write	01-Sep-21	9.3	Adobe Photoshop versions 21.2.10 (and earlier) and 22.4.3 (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 file. CVE ID : CVE-2021-36066	https://helpx .adobe.com/s ecurity/prod ucts/photosh op/apsb21- 68.html	O-MIC-WIND- 200921/2338
Improper Restriction of Operations within the Bounds of a Memory Buffer	01-Sep-21	9.3	Adobe Bridge version 11.1 (and earlier) is affected by a memory corruption vulnerability due to insecure handling of a malicious Bridge 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-2021-36067	https://helpx .adobe.com/s ecurity/prod ucts/bridge/ apsb21- 69.html	O-MIC-WIND- 200921/2339
CVSS Scoring Sc	cale 0-1	1-2	2-3 3-4 4-5 5-6	6-7 7-8	8-9 9-10

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Improper Restriction of Operations within the Bounds of a Memory Buffer	01-Sep-21	9.3	Adobe Bridge version 11.1 (and earlier) is affected by a memory corruption vulnerability due to insecure handling of a malicious Bridge 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-2021-36068	https://helpx .adobe.com/s ecurity/prod ucts/bridge/ apsb21- 69.html	O-MIC-WIND- 200921/2340
Improper Restriction of Operations within the Bounds of a Memory Buffer	01-Sep-21	9.3	Adobe Bridge version 11.1 (and earlier) is affected by a memory corruption vulnerability due to insecure handling of a malicious Bridge 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-2021-36069	https://helpx .adobe.com/s ecurity/prod ucts/bridge/ apsb21- 69.html	O-MIC-WIND- 200921/2341
Improper Restriction of Operations within the Bounds of a Memory Buffer	01-Sep-21	9.3	Adobe Media Encoder version 15.1 (and earlier) is affected by an improper memory access vulnerability when parsing a crafted .SVG file. An attacker could leverage this vulnerability to execute code 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-2021-36070	https://helpx .adobe.com/s ecurity/prod ucts/media- encoder/apsb 21-70.html	O-MIC-WIND- 200921/2342
	01-Sep-21	4.3	Adobe Bridge versions 11.1	https://helpx	O-MIC-WIND-

 3-4
 4-5
 5-6

 Page 940 of 1474

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
bounds Read			(and earlier) are affected by an out-of-bounds read vulnerability that could lead to disclosure of arbitrary memory. An attacker could leverage this vulnerability to bypass mitigations such as ASLR. Exploitation of this issue requires user interaction in that a victim must open a malicious file. CVE ID : CVE-2021-36071	.adobe.com/s ecurity/prod ucts/bridge/ apsb21- 69.html	200921/2343
			Adobe Bridge versions 11.1		
Out-of- bounds Write	01-Sep-21	9.3	(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 file.	https://helpx .adobe.com/s ecurity/prod ucts/bridge/ apsb21- 69.html	0-MIC-WIND- 200921/2344
			CVE ID : CVE-2021-36072		
Out-of- bounds Write	01-Sep-21	9.3	Adobe Bridge version 11.1 (and earlier) is affected by a heap-based buffer overflow vulnerability when parsing a crafted .SGI file. An attacker could leverage this vulnerability to execute code 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-2021-36073	https://helpx .adobe.com/s ecurity/prod ucts/bridge/ apsb21- 69.html	O-MIC-WIND- 200921/2345
0.1.5	01.6	4.3	Adobe Bridge versions 11.1	https://helpx	O-MIC-WIND-
Out-of-	01-Sep-21	T)	(and earlier) are affected by		200921/2346

3-4 4-5 Page 941 of 1474

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Read			an out-of-bounds read vulnerability that could lead to disclosure of arbitrary memory. An attacker could leverage this vulnerability to bypass mitigations such as ASLR. Exploitation of this issue requires user interaction in that a victim must open a malicious file. CVE ID : CVE-2021-36074	ecurity/prod ucts/bridge/ apsb21- 69.html	
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	01-Sep-21	9.3	Adobe Bridge version 11.1 (and earlier) is affected by a Buffer Overflow vulnerability due to insecure handling of a malicious Bridge 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-2021-36075	https://helpx .adobe.com/s ecurity/prod ucts/bridge/ apsb21- 69.html	O-MIC-WIND- 200921/2347
Improper Restriction of Operations within the Bounds of a Memory Buffer	01-Sep-21	9.3	Adobe Bridge version 11.1 (and earlier) is affected by a memory corruption vulnerability due to insecure handling of a malicious Bridge 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-2021-36076	https://helpx .adobe.com/s ecurity/prod ucts/bridge/ apsb21- 69.html	O-MIC-WIND- 200921/2348
Improper Restriction of	01-Sep-21	4.3	Adobe Bridge version 11.1 (and earlier) is affected by a memory corruption	https://helpx .adobe.com/s ecurity/prod	O-MIC-WIND- 200921/2349

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
Operations within the Bounds of a Memory Buffer			vulnerability due to insecure handling of a malicious SVG file, potentially resulting in local application denial of service in the context of the current user. User interaction is required to exploit this vulnerability. CVE ID : CVE-2021-36077	ucts/bridge/ apsb21- 69.html	
			Adobe Bridge version 11.1 (and earlier) is affected by a		
Improper Restriction of Operations within the Bounds of a Memory Buffer	01-Sep-21	9.3	memory corruption vulnerability due to insecure handling of a malicious Bridge file, potentially resulting in arbitrary code execution in the context of the current user. User interaction is required to exploit this vulnerability.	https://helpx .adobe.com/s ecurity/prod ucts/bridge/ apsb21- 69.html	O-MIC-WIND- 200921/2350
			CVE ID : CVE-2021-36078		
Out-of- bounds Read	01-Sep-21	9.3	Adobe Bridge version 11.1 (and earlier) is affected by an out-of-bounds read vulnerability when parsing a crafted .SGI file, which could result in a read past the end of an allocated memory structure. An attacker could leverage this vulnerability to execute code 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-2021-36079	https://helpx .adobe.com/s ecurity/prod ucts/bridge/ apsb21- 69.html	O-MIC-WIND- 200921/2351
Improper Privilege	06-Sep-21	4.6	Trend Micro Security (Consumer) 2021 and 2020	https://helpc enter.trendmi	0-MIC-WIND- 200921/2352
CVSS Scoring Sc	ale 0-1	1-2	2-3 3-4 4-5 5-6	6-7 7-8	8-9 9-10

Page 943 of 1474

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Managemen t			are vulnerable to a directory junction vulnerability which could allow an attacker to exploit the system to escalate privileges and create a denial of service.	cro.com/en- us/article/tm ka-10568	
			CVE ID : CVE-2021-36744		
Moxa	1			I	
oncell_g3470)a-lte-eu-t_fir	mware	9		
Improper Neutralizati on of Input During Web Page Generation ('Cross-site Scripting')	07-Sep-21	4.3	Certain MOXA devices allow reflected XSS via the Config Import menu. This affects WAC-2004 1.7, WAC-1001 2.1, WAC-1001-T 2.1, OnCell G3470A-LTE-EU 1.7, OnCell G3470A-LTE-EU 1.7, OnCell G3470A-LTE-EU-T 1.7, TAP- 323-EU-CT-T 1.3, TAP-323- US-CT-T 1.3, TAP-323-JP-CT- T 1.3, WDR-3124A-EU 2.3, WDR-3124A-EU-T 2.3, WDR- 3124A-US 2.3, and WDR- 3124A-US-T 2.3.	N/A	O-MOX-ONCE- 200921/2353
Improper Neutralizati on of Special Elements used in an OS Command ('OS Command Injection')	07-Sep-21	9	CVE ID : CVE-2021-39278 Certain MOXA devices allow Authenticated Command Injection via /forms/web_importTFTP. This affects WAC-2004 1.7, WAC-1001 2.1, WAC-1001-T 2.1, OnCell G3470A-LTE-EU 1.7, OnCell G3470A-LTE-EU T 1.7, TAP-323-EU-CT-T 1.3, TAP-323-US-CT-T 1.3, TAP- 323-JP-CT-T 1.3, WDR- 3124A-EU 2.3, WDR-3124A- EU-T 2.3, WDR-3124A-US 2.3, and WDR-3124A-US-T 2.3.	https://www. moxa.com	O-MOX-ONCE- 200921/2354
CVSS Scoring Sc	cale 0-1	1-2	2-3 3-4 4-5 5-6	6-7 7-8	8-9 9-10

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2021-39279		
oncell_g3470	a-lte-eu_firm	ware			
Improper Neutralizati on of Input During Web Page Generation ('Cross-site Scripting')	07-Sep-21	4.3	Certain MOXA devices allow reflected XSS via the Config Import menu. This affects WAC-2004 1.7, WAC-1001 2.1, WAC-1001-T 2.1, OnCell G3470A-LTE-EU 1.7, OnCell G3470A-LTE-EU-T 1.7, TAP- 323-EU-CT-T 1.3, TAP-323- US-CT-T 1.3, TAP-323-JP-CT- T 1.3, WDR-3124A-EU 2.3, WDR-3124A-EU-T 2.3, WDR- 3124A-US 2.3, and WDR- 3124A-US-T 2.3.	N/A	O-MOX-ONCE- 200921/2355
			CVE ID : CVE-2021-39278		
Improper Neutralizati on of Special Elements used in an OS Command ('OS Command Injection')	07-Sep-21	9	Certain MOXA devices allow Authenticated Command Injection via /forms/web_importTFTP. This affects WAC-2004 1.7, WAC-1001 2.1, WAC-1001-T 2.1, OnCell G3470A-LTE-EU 1.7, OnCell G3470A-LTE-EU T 1.7, TAP-323-EU-CT-T 1.3, TAP-323-US-CT-T 1.3, TAP- 323-JP-CT-T 1.3, WDR- 3124A-EU 2.3, WDR-3124A- EU-T 2.3, WDR-3124A-US 2.3, and WDR-3124A-US-T 2.3. CVE ID : CVE-2021-39279	https://www. moxa.com	O-MOX-ONCE- 200921/2356
tap-323-eu-c	t-t_firmware				<u> </u>
Improper Neutralizati on of Input During Web Page	07-Sep-21	4.3	Certain MOXA devices allow reflected XSS via the Config Import menu. This affects WAC-2004 1.7, WAC-1001 2.1, WAC-1001-T 2.1, OnCell	N/A	O-MOX-TAP 200921/2357
CVSS Scoring Sc	ale 0-1	1-2	2-3 3-4 4-5 5-6 Page 945 of 1474	6-7 7-8	8-9 9-10

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Generation ('Cross-site Scripting')			G3470A-LTE-EU 1.7, OnCell G3470A-LTE-EU-T 1.7, TAP- 323-EU-CT-T 1.3, TAP-323- US-CT-T 1.3, TAP-323-JP-CT- T 1.3, WDR-3124A-EU 2.3, WDR-3124A-EU-T 2.3, WDR- 3124A-US 2.3, and WDR- 3124A-US-T 2.3. CVE ID : CVE-2021-39278		
Improper Neutralizati on of Special Elements used in an OS Command ('OS Command Injection')	07-Sep-21	9	Certain MOXA devices allow Authenticated Command Injection via /forms/web_importTFTP. This affects WAC-2004 1.7, WAC-1001 2.1, WAC-1001-T 2.1, OnCell G3470A-LTE-EU 1.7, OnCell G3470A-LTE-EU T 1.7, TAP-323-EU-CT-T 1.3, TAP-323-US-CT-T 1.3, TAP- 323-JP-CT-T 1.3, WDR- 3124A-EU 2.3, WDR-3124A- EU-T 2.3, WDR-3124A-US 2.3, and WDR-3124A-US-T 2.3. CVE ID : CVE-2021-39279	https://www. moxa.com	0-MOX-TAP 200921/2358
tap-323-jp-ct	t-t_firmware				
Improper Neutralizati on of Input During Web Page Generation ('Cross-site Scripting')	07-Sep-21	4.3	Certain MOXA devices allow reflected XSS via the Config Import menu. This affects WAC-2004 1.7, WAC-1001 2.1, WAC-1001-T 2.1, OnCell G3470A-LTE-EU 1.7, OnCell G3470A-LTE-EU-T 1.7, TAP- 323-EU-CT-T 1.3, TAP-323- US-CT-T 1.3, TAP-323-JP-CT- T 1.3, WDR-3124A-EU 2.3, WDR-3124A-EU-T 2.3, WDR- 3124A-US 2.3, and WDR-	N/A	0-MOX-TAP 200921/2359

CVSS Scoring Scale	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10
			Р	age 946 c	of 1474					

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			3124A-US-T 2.3.		
			CVE ID : CVE-2021-39278		
Improper Neutralizati on of Special Elements used in an OS Command ('OS Command Injection')	07-Sep-21	9	Certain MOXA devices allow Authenticated Command Injection via /forms/web_importTFTP. This affects WAC-2004 1.7, WAC-1001 2.1, WAC-1001-T 2.1, OnCell G3470A-LTE-EU 1.7, OnCell G3470A-LTE-EU- T 1.7, TAP-323-EU-CT-T 1.3, TAP-323-US-CT-T 1.3, TAP- 323-JP-CT-T 1.3, WDR- 3124A-EU 2.3, WDR-3124A- EU-T 2.3, WDR-3124A-US 2.3, and WDR-3124A-US-T 2.3.	https://www. moxa.com	0-MOX-TAP 200921/2360
			CVE ID : CVE-2021-39279		
tap-323-us-c	t-t_firmware				
Improper Neutralizati on of Input During Web Page Generation ('Cross-site Scripting')	07-Sep-21	4.3	Certain MOXA devices allow reflected XSS via the Config Import menu. This affects WAC-2004 1.7, WAC-1001 2.1, WAC-1001-T 2.1, OnCell G3470A-LTE-EU 1.7, OnCell G3470A-LTE-EU-T 1.7, TAP- 323-EU-CT-T 1.3, TAP-323- US-CT-T 1.3, TAP-323-JP-CT- T 1.3, WDR-3124A-EU 2.3, WDR-3124A-EU-T 2.3, WDR- 3124A-US 2.3, and WDR- 3124A-US-T 2.3.	N/A	O-MOX-TAP 200921/2361
Improper			CVE ID : CVE-2021-39278 Certain MOXA devices allow		
Improper Neutralizati on of Special Elements used in an	07-Sep-21	9	Certain MOXA devices allow Authenticated Command Injection via /forms/web_importTFTP. This affects WAC-2004 1.7,	https://www. moxa.com	O-MOX-TAP 200921/2362
CVSS Scoring Sc	ale 0-1	1-2	2-3 3-4 4-5 5-6	6-7 7-8	8-9 9-10

OS Command ('OS Command Injection')Image: Command Command ('OS Command Injection')Image: Command	Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Improper Neutralizati on of Input During Web Page Generation ('Cross-site Scripting')07-Sep-214.3Certain MOXA devices allow reflected XSS via the Config Import menu. This affects (3470A-LTE-EU 1.7, OnCell G3470A-LTE-EU 1.7, OnCell G3470A-LTE-EU-T 1.3, TAP-323-IP-CT- T 1.3, WDR-3124A-EU 2.3, WDR-3124A-EU 2.3, WDR- 3124A-US 2.3, and WDR- Authenticated Command Injection via (Or (OS <td>Command ('OS Command</td> <td></td> <td></td> <td>2.1, OnCell G3470A-LTE-EU 1.7, OnCell G3470A-LTE-EU- T 1.7, TAP-323-EU-CT-T 1.3, TAP-323-US-CT-T 1.3, TAP- 323-JP-CT-T 1.3, WDR- 3124A-EU 2.3, WDR-3124A- EU-T 2.3, WDR-3124A-US 2.3, and WDR-3124A-US-T 2.3.</td> <td></td> <td></td>	Command ('OS Command			2.1, OnCell G3470A-LTE-EU 1.7, OnCell G3470A-LTE-EU- T 1.7, TAP-323-EU-CT-T 1.3, TAP-323-US-CT-T 1.3, TAP- 323-JP-CT-T 1.3, WDR- 3124A-EU 2.3, WDR-3124A- EU-T 2.3, WDR-3124A-US 2.3, and WDR-3124A-US-T 2.3.		
Improper Neutralizati on of Input During Web Page Generation ('Cross-site Scripting')of-sep-21ess Pase ('A-A) 	wac-1001-t_f	irmware				
Improper Neutralizati on of Special Elements used in an OS Command ('OS Command Injection')Authenticated Command Injection via /forms/web_importTFTP. This affects WAC-2004 1.7, WAC-1001 2.1, WAC-1001-T 2.1, OnCell G3470A-LTE-EU- T 1.7, TAP-323-EU-CT-T 1.3, TAP- 323-JP-CT-T 1.3, WDR- 3124A-EU 2.3, WDR-3124A-https://www. noxa.comO-MOX-WAC 200921/2364	Neutralizati on of Input During Web Page Generation ('Cross-site	07-Sep-21	4.3	reflected XSS via the Config Import menu. This affects WAC-2004 1.7, WAC-1001 2.1, WAC-1001-T 2.1, OnCell G3470A-LTE-EU 1.7, OnCell G3470A-LTE-EU-T 1.7, TAP- 323-EU-CT-T 1.3, TAP-323- US-CT-T 1.3, TAP-323-JP-CT- T 1.3, WDR-3124A-EU 2.3, WDR-3124A-EU-T 2.3, WDR- 3124A-US 2.3, and WDR- 3124A-US-T 2.3.	N/A	
	Neutralizati on of Special Elements used in an OS Command ('OS Command	07-Sep-21	9	Authenticated Command Injection via /forms/web_importTFTP. This affects WAC-2004 1.7, WAC-1001 2.1, WAC-1001-T 2.1, OnCell G3470A-LTE-EU 1.7, OnCell G3470A-LTE-EU- T 1.7, TAP-323-EU-CT-T 1.3, TAP-323-US-CT-T 1.3, TAP- 323-JP-CT-T 1.3, WDR- 3124A-EU 2.3, WDR-3124A-		

Page 948 of 1474

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			2.3, and WDR-3124A-US-T 2.3.		
			2.3. CVE ID : CVE-2021-39279		
wac-1001_fir	mware				
Improper Neutralizati on of Input During Web Page Generation ('Cross-site Scripting')	07-Sep-21	4.3	Certain MOXA devices allow reflected XSS via the Config Import menu. This affects WAC-2004 1.7, WAC-1001 2.1, WAC-1001-T 2.1, OnCell G3470A-LTE-EU 1.7, OnCell G3470A-LTE-EU-T 1.7, TAP- 323-EU-CT-T 1.3, TAP-323- US-CT-T 1.3, TAP-323-JP-CT- T 1.3, WDR-3124A-EU 2.3, WDR-3124A-EU-T 2.3, WDR- 3124A-US 2.3, and WDR- 3124A-US-T 2.3.	N/A	0-MOX-WAC 200921/2365
			CVE ID : CVE-2021-39278		
Improper Neutralizati on of Special Elements used in an OS Command ('OS Command Injection')	07-Sep-21	9	Certain MOXA devices allow Authenticated Command Injection via /forms/web_importTFTP. This affects WAC-2004 1.7, WAC-1001 2.1, WAC-1001-T 2.1, OnCell G3470A-LTE-EU 1.7, OnCell G3470A-LTE-EU- T 1.7, TAP-323-EU-CT-T 1.3, TAP-323-US-CT-T 1.3, TAP- 323-JP-CT-T 1.3, WDR- 3124A-EU 2.3, WDR-3124A- EU-T 2.3, WDR-3124A-US 2.3, and WDR-3124A-US-T 2.3. CVE ID : CVE-2021-39279	https://www. moxa.com	0-MOX-WAC 200921/2366
wac-2004_firmware					
Improper Neutralizati on of Input	07-Sep-21	4.3	Certain MOXA devices allow reflected XSS via the Config Import menu. This affects	N/A	0-MOX-WAC 200921/2367
CVSS Scoring Sc	ale 0-1	1-2	2-3 3-4 4-5 5-6 Page 949 of 1474	6-7 7-8	8-9 9-10

Page 949 of 1474

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
During Web Page Generation ('Cross-site Scripting')			WAC-2004 1.7, WAC-1001 2.1, WAC-1001-T 2.1, OnCell G3470A-LTE-EU 1.7, OnCell G3470A-LTE-EU-T 1.7, TAP- 323-EU-CT-T 1.3, TAP-323- US-CT-T 1.3, TAP-323-JP-CT- T 1.3, WDR-3124A-EU 2.3, WDR-3124A-EU-T 2.3, WDR- 3124A-US 2.3, and WDR- 3124A-US-T 2.3. CVE ID : CVE-2021-39278		
Improper Neutralizati on of Special Elements used in an OS Command ('OS Command Injection')	07-Sep-21	9	Certain MOXA devices allow Authenticated Command Injection via /forms/web_importTFTP. This affects WAC-2004 1.7, WAC-1001 2.1, WAC-1001-T 2.1, OnCell G3470A-LTE-EU 1.7, OnCell G3470A-LTE-EU T 1.7, TAP-323-EU-CT-T 1.3, TAP-323-US-CT-T 1.3, TAP- 323-JP-CT-T 1.3, WDR- 3124A-EU 2.3, WDR-3124A- EU-T 2.3, WDR-3124A-US 2.3, and WDR-3124A-US-T 2.3. CVE ID : CVE-2021-39279	https://www. moxa.com	0-MOX-WAC 200921/2368
wdr-3124a-e	u-t_firmware	2			
Improper Neutralizati on of Input During Web Page Generation ('Cross-site Scripting')	07-Sep-21	4.3	Certain MOXA devices allow reflected XSS via the Config Import menu. This affects WAC-2004 1.7, WAC-1001 2.1, WAC-1001-T 2.1, OnCell G3470A-LTE-EU 1.7, OnCell G3470A-LTE-EU-T 1.7, TAP- 323-EU-CT-T 1.3, TAP-323- US-CT-T 1.3, TAP-323-JP-CT- T 1.3, WDR-3124A-EU 2.3, WDR-3124A-EU-T 2.3, WDR-	N/A	0-MOX-WDR- - 200921/2369
CVSS Scoring Sc	ale 0-1	1-2	2-3 3-4 4-5 5-6 Page 950 of 1474	6-7 7-8	8-9 9-10

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			3124A-US 2.3, and WDR- 3124A-US-T 2.3.		
			CVE ID : CVE-2021-39278		
Improper Neutralizati on of Special Elements used in an OS Command ('OS Command Injection')	07-Sep-21	9	Certain MOXA devices allow Authenticated Command Injection via /forms/web_importTFTP. This affects WAC-2004 1.7, WAC-1001 2.1, WAC-1001-T 2.1, OnCell G3470A-LTE-EU 1.7, OnCell G3470A-LTE-EU T 1.7, TAP-323-EU-CT-T 1.3, TAP-323-US-CT-T 1.3, TAP- 323-JP-CT-T 1.3, WDR- 3124A-EU 2.3, WDR-3124A- EU-T 2.3, WDR-3124A-US 2.3, and WDR-3124A-US-T 2.3.	https://www. moxa.com	O-MOX-WDR- - 200921/2370
			CVE ID : CVE-2021-39279		
wdr-3124a-e	eu_firmware				
Improper Neutralizati on of Input During Web Page Generation ('Cross-site Scripting')	07-Sep-21	4.3	Certain MOXA devices allow reflected XSS via the Config Import menu. This affects WAC-2004 1.7, WAC-1001 2.1, WAC-1001-T 2.1, OnCell G3470A-LTE-EU 1.7, OnCell G3470A-LTE-EU-T 1.7, TAP- 323-EU-CT-T 1.3, TAP-323- US-CT-T 1.3, TAP-323-JP-CT- T 1.3, WDR-3124A-EU 2.3, WDR-3124A-EU-T 2.3, WDR- 3124A-US 2.3, and WDR- 3124A-US-T 2.3. CVE ID : CVE-2021-39278	N/A	O-MOX-WDR- - 200921/2371
Improper			Certain MOXA devices allow	https://www.	O-MOX-WDR-
Neutralizati on of Special	07-Sep-21	9	Authenticated Command Injection via /forms/web_importTFTP.	https://www. moxa.com	- 200921/2372

used in an					
OS Command ('OS Command Injection')			This affects WAC-2004 1.7, WAC-1001 2.1, WAC-1001-T 2.1, OnCell G3470A-LTE-EU 1.7, OnCell G3470A-LTE-EU- T 1.7, TAP-323-EU-CT-T 1.3, TAP-323-US-CT-T 1.3, TAP- 323-JP-CT-T 1.3, WDR- 3124A-EU 2.3, WDR-3124A- EU-T 2.3, WDR-3124A-US 2.3, and WDR-3124A-US-T 2.3. CVE ID : CVE-2021-39279		
wdr-3124a-u	s-t_firmware				
Improper Neutralizati on of Input During Web Page Generation ('Cross-site Scripting')	07-Sep-21	4.3	Certain MOXA devices allow reflected XSS via the Config Import menu. This affects WAC-2004 1.7, WAC-1001 2.1, WAC-1001-T 2.1, OnCell G3470A-LTE-EU 1.7, OnCell G3470A-LTE-EU-T 1.7, TAP- 323-EU-CT-T 1.3, TAP-323- US-CT-T 1.3, TAP-323-JP-CT- T 1.3, WDR-3124A-EU 2.3, WDR-3124A-EU-T 2.3, WDR- 3124A-US 2.3, and WDR- 3124A-US-T 2.3. CVE ID : CVE-2021-39278	N/A	O-MOX-WDR- - 200921/2373
Improper Neutralizati on of Special Elements used in an OS Command ('OS Command Injection')	07-Sep-21	9	Certain MOXA devices allow Authenticated Command Injection via /forms/web_importTFTP. This affects WAC-2004 1.7, WAC-1001 2.1, WAC-1001-T 2.1, OnCell G3470A-LTE-EU 1.7, OnCell G3470A-LTE-EU T 1.7, TAP-323-EU-CT-T 1.3, TAP-323-US-CT-T 1.3, TAP- 323-JP-CT-T 1.3, WDR- 3124A-EU 2.3, WDR-3124A-	https://www. moxa.com	O-MOX-WDR- - 200921/2374

Page 952 of 1474

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID		
			EU-T 2.3, WDR-3124A-US 2.3, and WDR-3124A-US-T 2.3.				
wdr-3124a-u	c firmwara		CVE ID : CVE-2021-39279				
wur-5124a-u	is_infiniware		Contain MOVA deviace allow				
Improper Neutralizati on of Input During Web Page Generation ('Cross-site Scripting')	07-Sep-21	4.3	Certain MOXA devices allow reflected XSS via the Config Import menu. This affects WAC-2004 1.7, WAC-1001 2.1, WAC-1001-T 2.1, OnCell G3470A-LTE-EU 1.7, OnCell G3470A-LTE-EU-T 1.7, TAP- 323-EU-CT-T 1.3, TAP-323- US-CT-T 1.3, TAP-323-JP-CT- T 1.3, WDR-3124A-EU 2.3, WDR-3124A-EU-T 2.3, WDR- 3124A-US 2.3, and WDR- 3124A-US-T 2.3. CVE ID : CVE-2021-39278	N/A	O-MOX-WDR- - 200921/2375		
Improper Neutralizati on of Special Elements used in an OS Command ('OS Command Injection')	07-Sep-21	9	Certain MOXA devices allow Authenticated Command Injection via /forms/web_importTFTP. This affects WAC-2004 1.7, WAC-1001 2.1, WAC-1001-T 2.1, OnCell G3470A-LTE-EU 1.7, OnCell G3470A-LTE-EU- T 1.7, TAP-323-EU-CT-T 1.3, TAP-323-US-CT-T 1.3, TAP- 323-JP-CT-T 1.3, WDR- 3124A-EU 2.3, WDR-3124A- EU-T 2.3, WDR-3124A-US 2.3, and WDR-3124A-US-T 2.3. CVE ID : CVE-2021-39279	https://www. moxa.com	O-MOX-WDR- - 200921/2376		
Paloaltonetworks							
pan-os							

0-1

1-2

2-3

3-4 Page 953 of 1474

4-5

5-6

6-7

7-8

8-9

Improper Neutralizati on of Input During Web Page Generation ('Cross-site Scripting')08-Sep-213.5A reflected cross-site scripting (XSS) vulnerability in the Palo Alto Network PAN-OS web interface enables an authenticated PAN-OS administrator to click on a specially crafted link that performs arbitrary actions in the PAN-OS web interface as the PAN-OS web interface as the PAN-OS Neutralizati or of Input During Web Page Generation ('Cross-site Scripting')08-Sep-213.5A reflected cross-site scripting'https://secur ity.paloaltone tworks.com/ CVE-2021- 30520-PAL-PAN 200921/2377 3052Time-of- check Time-of- check Time-of- condition8.5A time-of-Get to time-of- user (TOCTOU) race condition vulnerability in the Palo Alto Networks PAN-OS 8.1 versions earlier than 9.1.0; PAN-OS to versions earlier than authenticated administrator with permission to upload plugins to execute arbitrary conditionhttps://secur ity.paloaltone tworks.com/ CVE-2021-30520-PAL-PAN 200921/2378 3054Time-of- check Time-of- check	Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Time-of- check Time- of-use (TOCTOU)08-Sep-218.58.5use (TOCTOU) race condition vulnerability in the Palo Alto Networks PAN-OS web interface enables an authenticated administrator plugins to execute arbitrary ocde with root user privileges. This issue impacts: PAN-OS 8.1 versions earlier than PAN-OS 8.1.20; PAN-OS 9.0.14; PAN-OS 9.1 versions earlier than PAN-OS 9.0.14; PAN-OS 1.11; PAN-OS 10.0https://seur https://seur interface https://seur interface https://seur interface interface interface enables an authenticated administrator privileges. This issue impacts: PAN-OS 8.1.20; PAN-OS 9.0.14; PAN-OS 9.1 versions earlier than PAN-OS 9.0.14; PAN-OS 1.11; PAN-OS 10.0https://seur https://seur interface<	Neutralizati on of Input During Web Page Generation ('Cross-site	08-Sep-21	3.5	scripting (XSS) vulnerability in the Palo Alto Network PAN-OS web interface enables an authenticated network-based attacker to mislead another authenticated PAN-OS administrator to click on a specially crafted link that performs arbitrary actions in the PAN-OS web interface as the targeted authenticated administrator. This issue impacts: PAN-OS 8.1 versions earlier than 8.1.20; PAN-OS 9.0 versions earlier than 9.0.14; PAN-OS 9.1 versions earlier than 9.1.10; PAN-OS 10.0 versions earlier than 10.0.2. This issue does not affect Prisma Access.	ity.paloaltone tworks.com/ CVE-2021-	
	check Time- of-use (TOCTOU) Race	08-Sep-21	8.5	use (TOCTOU) race condition vulnerability in the Palo Alto Networks PAN-OS web interface enables an authenticated administrator with permission to upload plugins to execute arbitrary code with root user privileges. This issue impacts: PAN-OS 8.1 versions earlier than PAN-OS 8.1.20; PAN-OS 9.0 versions earlier than PAN-OS 9.0.14; PAN-OS 9.1 versions earlier than PAN-OS 9.1.11; PAN-OS 10.0	ity.paloaltone tworks.com/ CVE-2021-	

Page 954 of 1474

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID			
			10.0.7; PAN-OS 10.1 versions earlier than PAN-OS 10.1.2. This issue does not affect Prisma Access.					
			CVE ID : CVE-2021-3054					
Qualcomm	I			I				
apq8009w_fi	apq8009w_firmware							
Exposure of Resource to Wrong Sphere	08-Sep-21	2.1	Child process can leak information from parent process due to numeric pids are getting compared and these pid can be reused in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wearables	https://www. qualcomm.co m/company/ product- security/bull etins/august- 2021-bulletin	0-QUA-APQ8- 200921/2379			
			CVE ID : CVE-2021-1904					
Loop with Unreachable Exit Condition ('Infinite Loop')	08-Sep-21	5	Loop with unreachable exit condition may occur due to improper handling of unsupported input in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Voice & Music, Snapdragon Wearables CVE ID : CVE-2021-1914	https://www. qualcomm.co m/company/ product- security/bull etins/august- 2021-bulletin	0-QUA-APQ8- 200921/2380			
Out-of- bounds Write	08-Sep-21	10	Possible buffer underflow due to lack of check for negative indices values when processing user provided	https://www. qualcomm.co m/company/ product-	0-QUA-APQ8- 200921/2381			

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			input in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Voice & Music, Snapdragon Wearables	security/bull etins/august- 2021-bulletin	
			CVE ID : CVE-2021-1916		
Integer Underflow (Wrap or Wraparoun d)	08-Sep-21	10	Integer underflow can occur when the RTCP length is lesser than than the actual blocks present in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Voice & Music, Snapdragon Wearables	https://www. qualcomm.co m/company/ product- security/bull etins/august- 2021-bulletin	O-QUA-APQ8- 200921/2382
			CVE ID : CVE-2021-1919 Integer underflow can occur		
Integer Underflow (Wrap or Wraparoun d)	08-Sep-21	10	due to improper handling of incoming RTCP packets in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Voice & Music, Snapdragon Wearables	https://www. qualcomm.co m/company/ product- security/bull etins/august- 2021-bulletin	0-QUA-APQ8- 200921/2383
Duffer Car			CVE ID : CVE-2021-1920	https://-	
Buffer Copy without Checking Size of Input ('Classic	08-Sep-21	10	Possible buffer overflow due to improper validation of device types during P2P search in Snapdragon Auto, Snapdragon Compute,	https://www. qualcomm.co m/company/ product- security/bull	0-QUA-APQ8- 200921/2384

0-1

1-2

2-3 3-4

Page 956 of 1474

4-5

5-6

6-7

7-8

8-9

Buffer Overflow')ether Snapdragon Consumer 10T, Snapdragon Industrial 10T, Snapdragon Mobile, Snapdragon Worde Infrastructure and Networkingetins/august- 2021-bulletinapq8009_firmate Exposure of Resource to Wrong Sphere08-Sep-212.1Child process can leak information from parent process due to numeric pids are getting compared and these pid can be reused in Snapdragon Mobile, Snapdragon Consumer 10T, Networkinghttps://www. qualcomm.co m/company/ product- security/bull etins/august- 2021-bulletinSphere08-Sep-212.1Child process can leak information from parent process due to numeric pids are getting compared and these pid can be reused in Snapdragon Compute, Snapdragon Compute, Snapdragon Mobile, Snapdragon Mobile, Snapdragon Mobile, Snapdragon Outce & Music, Snapdragon Mobile, Snapdragon Outce & Music, Snapdragon Compute, Snapdragon Auto, Snapdragon Auto, Snapdragon Mobile, Snapdragon	Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Exposure of Resource to Wrong Sphere08-Sep-212.1Child process can leak information from parent process due to numeric pids are getting compared and these pid can be reused in Snapdragon Connectivity, Snapdragon Consumer 10T, Snapdragon Industrial I0T, Snapdragon Nobile, Snapdragon Wearableshttps://www. qualcomm.co m/company/ product- security/bull etins/august- 2021-bulletin0-QUA-APQ8- 200921/2385Loop with Unreachable Exit Condition ('Infinite Loop')08-Sep-215Loop with unreachable exit condition may occur due to improper handling of unsupported input in Snapdragon Consumer 10T, Snapdragon Compute, Snapdragon Compute, Snapdragon Consumer 10T, Snapdragon Consumer 10T, Snapdragon Compute, Snapdragon Compute, Snapdragon Mearableshttps://www. qualcomm.co m/company/ product- security/bull etins/august- 201-bulletin0-QUA-APQ8- 200921/2385Loop with Unreachable Exit Condition ('Infinite Loop')8-Sep-215Loop with unreachable exit condition may occur due to improper handling of unsupported input in Snapdragon Connectivity, Snapdragon Consumer 10T, Snapdragon Industrial 10				Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking		
Exposure of Resource to Wrong Sphereendefinition Passesinformation from parent process due to numeric pids are getting compared and these pid can be reused in Snapdragon Compute, Snapdragon Consumer IOT, Snapdragon Industrial IOT Snapdragon Mobile, Snapdragon Mobile, Snapdragon Mobile, Snapdragon Wearableshttps://www. product- security/bull etins/august- 201-bulletinoutput product- security/bull etins/august- 	apq8009_firm	nware				
Loop with Unreachable Exit ConditionLoop with unreachable exit condition may occur due to improper handling of unsupported input in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Industrial IOT, Snapdragon Industrial IOT, Snapdragon Industrial IOT, Napdragon Industrial IOT, Voice & Music, Snapdragon Wearableshttps://www. qualcomm.co m/company/ etins/august- 2021-bulletinPole pole product- security/bull etins/august- 2021-bulletin	Resource to Wrong	08-Sep-21	2.1	information from parent process due to numeric pids are getting compared and these pid can be reused in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music,	qualcomm.co m/company/ product- security/bull etins/august-	с с
	Unreachable Exit Condition ('Infinite	08-Sep-21	5	Loop with unreachable exit condition may occur due to improper handling of unsupported input in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Voice & Music, Snapdragon Wearables	qualcomm.co m/company/ product- security/bull etins/august-	• •

 3-4
 4-5
 5-6
 6-7

 Page 957 of 1474

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Out-of- bounds Write	08-Sep-21	10	Possible buffer underflow due to lack of check for negative indices values when processing user provided input in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Voice & Music, Snapdragon Wearables CVE ID : CVE-2021-1916	https://www. qualcomm.co m/company/ product- security/bull etins/august- 2021-bulletin	O-QUA-APQ8- 200921/2387
Integer Underflow (Wrap or Wraparoun d)	08-Sep-21	10	Integer underflow can occur when the RTCP length is lesser than than the actual blocks present in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Voice & Music, Snapdragon Wearables CVE ID : CVE-2021-1919	https://www. qualcomm.co m/company/ product- security/bull etins/august- 2021-bulletin	0-QUA-APQ8- 200921/2388
Integer Underflow (Wrap or Wraparoun d)	08-Sep-21	10	Integer underflow can occur due to improper handling of incoming RTCP packets in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Voice & Music, Snapdragon Wearables	https://www. qualcomm.co m/company/ product- security/bull etins/august- 2021-bulletin	O-QUA-APQ8- 200921/2389
Out-of-	08-Sep-21	3.6	CVE ID : CVE-2021-1920 Buffer over read could occur	https://www.	0-QUA-APQ8-
	00 00p =1	0.0	Duffel Over leau could occur		0-007-71 00-

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
bounds Read			due to incorrect check of buffer size while flashing emmc devices in Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking	qualcomm.co m/company/ product- security/bull etins/august- 2021-bulletin	200921/2390
			CVE ID : CVE-2021-1928		
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	08-Sep-21	10	Possible buffer overflow due to improper validation of device types during P2P search in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Woice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking	https://www. qualcomm.co m/company/ product- security/bull etins/august- 2021-bulletin	O-QUA-APQ8- 200921/2391
			CVE ID : CVE-2021-1972		
apq8017_firm	nware				
Exposure of Resource to Wrong Sphere	08-Sep-21	2.1	Child process can leak information from parent process due to numeric pids are getting compared and these pid can be reused in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile,	https://www. qualcomm.co m/company/ product- security/bull etins/august- 2021-bulletin	0-QUA-APQ8- 200921/2392
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 & CVE ID	Patch	NCIIPC ID
			Snapdragon Voice & Music, Snapdragon Wearables		
			CVE ID : CVE-2021-1904		
Loop with Unreachable Exit Condition ('Infinite Loop')	08-Sep-21	5	Loop with unreachable exit condition may occur due to improper handling of unsupported input in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Voice & Music, Snapdragon Wearables CVE ID : CVE-2021-1914	https://www. qualcomm.co m/company/ product- security/bull etins/august- 2021-bulletin	0-QUA-APQ8- 200921/2393
Out-of- bounds Write	08-Sep-21	10	Possible buffer underflow due to lack of check for negative indices values when processing user provided input in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Voice & Music, Snapdragon Wearables CVE ID : CVE-2021-1916	https://www. qualcomm.co m/company/ product- security/bull etins/august- 2021-bulletin	O-QUA-APQ8- 200921/2394
Integer Underflow (Wrap or Wraparoun d)	08-Sep-21	10	Integer underflow can occur when the RTCP length is lesser than than the actual blocks present in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon	https://www. qualcomm.co m/company/ product- security/bull etins/august- 2021-bulletin	O-QUA-APQ8- 200921/2395

1-2

0-1

5-6

6-7

7-8

8-9

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Voice & Music, Snapdragon Wearables CVE ID : CVE-2021-1919		
Integer Underflow (Wrap or Wraparoun d)	08-Sep-21	10	Integer underflow can occur due to improper handling of incoming RTCP packets in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Voice & Music, Snapdragon Wearables	https://www. qualcomm.co m/company/ product- security/bull etins/august- 2021-bulletin	0-QUA-APQ8- 200921/2396
			CVE ID : CVE-2021-1920		
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	08-Sep-21	10	Possible buffer overflow due to improper validation of device types during P2P search in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Woice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking CVE ID : CVE-2021-1972	https://www. qualcomm.co m/company/ product- security/bull etins/august- 2021-bulletin	0-QUA-APQ8- 200921/2397
apq8037_firm	nware				
Loop with Unreachable Exit Condition ('Infinite Loop')	08-Sep-21	5	Loop with unreachable exit condition may occur due to improper handling of unsupported input in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity,	https://www. qualcomm.co m/company/ product- security/bull etins/august- 2021-bulletin	0-QUA-APQ8- 200921/2398
CVSS Scoring Sca	ale 0-1	1-2	2-3 3-4 4-5 5-6 Page 961 of 1474	6-7 7-8	8-9 9-10

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Voice & Music, Snapdragon Wearables CVE ID : CVE-2021-1914		
Out-of- bounds Write	08-Sep-21	10	Possible buffer underflow due to lack of check for negative indices values when processing user provided input in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Voice & Music, Snapdragon Wearables CVE ID : CVE-2021-1916	https://www. qualcomm.co m/company/ product- security/bull etins/august- 2021-bulletin	0-QUA-APQ8- 200921/2399
Integer Underflow (Wrap or Wraparoun d)	08-Sep-21	10	Integer underflow can occur when the RTCP length is lesser than than the actual blocks present in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Voice & Music, Snapdragon Wearables CVE ID : CVE-2021-1919	https://www. qualcomm.co m/company/ product- security/bull etins/august- 2021-bulletin	0-QUA-APQ8- 200921/2400
Integer Underflow (Wrap or Wraparoun d)	08-Sep-21	10	Integer underflow can occur due to improper handling of incoming RTCP packets in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT,	https://www. qualcomm.co m/company/ product- security/bull etins/august- 2021-bulletin	0-QUA-APQ8- 200921/2401
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 Industrial IOT, Snapdragon IoT, Snapdragon Voice & Music, Snapdragon Wearables		
			CVE ID : CVE-2021-1920		
apq8053_firm	nware				
Exposure of Resource to Wrong Sphere	08-Sep-21	2.1	Child process can leak information from parent process due to numeric pids are getting compared and these pid can be reused in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wearables CVE ID : CVE-2021-1904	https://www. qualcomm.co m/company/ product- security/bull etins/august- 2021-bulletin	0-QUA-APQ8- 200921/2402
Loop with Unreachable Exit Condition ('Infinite Loop')	08-Sep-21	5	Loop with unreachable exit condition may occur due to improper handling of unsupported input in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Voice & Music, Snapdragon Wearables CVE ID : CVE-2021-1914	https://www. qualcomm.co m/company/ product- security/bull etins/august- 2021-bulletin	O-QUA-APQ8- 200921/2403
Out-of- bounds Write	08-Sep-21	10	Possible buffer underflow due to lack of check for negative indices values when processing user provided input in Snapdragon Auto,	https://www. qualcomm.co m/company/ product- security/bull	O-QUA-APQ8- 200921/2404
CVSS Scoring Sc	ale 0-1	1-2	2-3 3-4 4-5 5-6	6-7 7-8	8-9 9-10

Page 963 of 1474

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Voice & Music, Snapdragon Wearables	etins/august- 2021-bulletin	
			CVE ID : CVE-2021-1916		
Integer Underflow (Wrap or Wraparoun d)	08-Sep-21	10	Integer underflow can occur when the RTCP length is lesser than than the actual blocks present in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Voice & Music, Snapdragon Wearables	https://www. qualcomm.co m/company/ product- security/bull etins/august- 2021-bulletin	O-QUA-APQ8- 200921/2405
			CVE ID : CVE-2021-1919		
Integer Underflow (Wrap or Wraparoun d)	08-Sep-21	10	Integer underflow can occur due to improper handling of incoming RTCP packets in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Voice & Music, Snapdragon Wearables	https://www. qualcomm.co m/company/ product- security/bull etins/august- 2021-bulletin	O-QUA-APQ8- 200921/2406
			CVE ID : CVE-2021-1920		
Out-of- bounds Read	08-Sep-21	3.6	Buffer over read could occur due to incorrect check of buffer size while flashing emmc devices in Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon	https://www. qualcomm.co m/company/ product- security/bull etins/august-	O-QUA-APQ8- 200921/2407

0-1

1-2

7-8

5-6

6-7

8-9

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking	2021-bulletin	
			CVE ID : CVE-2021-1928		
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	08-Sep-21	10	Possible buffer overflow due to improper validation of device types during P2P search in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Woice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking CVE ID : CVE-2021-1972	https://www. qualcomm.co m/company/ product- security/bull etins/august- 2021-bulletin	O-QUA-APQ8- 200921/2408
apq8064au_f	irmware				
Exposure of Resource to Wrong Sphere	08-Sep-21	2.1	Child process can leak information from parent process due to numeric pids are getting compared and these pid can be reused in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wearables CVE ID : CVE-2021-1904	https://www. qualcomm.co m/company/ product- security/bull etins/august- 2021-bulletin	0-QUA-APQ8- 200921/2409
				1	1

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
without Checking Size of Input ('Classic Buffer Overflow')			to improper validation of device types during P2P search in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Woice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking CVE ID : CVE-2021-1972	qualcomm.co m/company/ product- security/bull etins/august- 2021-bulletin	200921/2410
apq8076_firr	nware				
Exposure of Resource to Wrong Sphere	08-Sep-21	2.1	Child process can leak information from parent process due to numeric pids are getting compared and these pid can be reused in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wearables CVE ID : CVE-2021-1904	https://www. qualcomm.co m/company/ product- security/bull etins/august- 2021-bulletin	O-QUA-APQ8- 200921/2411
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	08-Sep-21	10	Possible buffer overflow due to improper validation of device types during P2P search in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music,	https://www. qualcomm.co m/company/ product- security/bull etins/august- 2021-bulletin	0-QUA-APQ8- 200921/2412

			0 1		
			Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking		
			CVE ID : CVE-2021-1972		
apq8084_firm	iware				
Out-of- bounds Write	08-Sep-21	10	Possible buffer underflow due to lack of check for negative indices values when processing user provided input in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Voice & Music, Snapdragon Wearables CVE ID : CVE-2021-1916	https://www. qualcomm.co m/company/ product- security/bull etins/august- 2021-bulletin	0-QUA-APQ8- 200921/2413
Integer Underflow (Wrap or Wraparoun d)	08-Sep-21	10	Integer underflow can occur when the RTCP length is lesser than than the actual blocks present in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Voice & Music, Snapdragon Wearables CVE ID : CVE-2021-1919	https://www. qualcomm.co m/company/ product- security/bull etins/august- 2021-bulletin	0-QUA-APQ8- 200921/2414
Integer Underflow (Wrap or Wraparoun d)	08-Sep-21	10	Integer underflow can occur due to improper handling of incoming RTCP packets in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT,	https://www. qualcomm.co m/company/ product- security/bull etins/august- 2021-bulletin	0-QUA-APQ8- 200921/2415

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Voice & Music, Snapdragon Wearables		
			CVE ID : CVE-2021-1920		
apq8096au_f	firmware				
Exposure of Resource to Wrong Sphere	08-Sep-21	2.1	Child process can leak information from parent process due to numeric pids are getting compared and these pid can be reused in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wearables CVE ID : CVE-2021-1904	https://www. qualcomm.co m/company/ product- security/bull etins/august- 2021-bulletin	0-QUA-APQ8- 200921/2416
Loop with Unreachable Exit Condition ('Infinite Loop')	08-Sep-21	5	Loop with unreachable exit condition may occur due to improper handling of unsupported input in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Voice & Music, Snapdragon Wearables CVE ID : CVE-2021-1914	https://www. qualcomm.co m/company/ product- security/bull etins/august- 2021-bulletin	O-QUA-APQ8- 200921/2417
Out-of- bounds Write	08-Sep-21	10	Possible buffer underflow due to lack of check for negative indices values when processing user provided input in Snapdragon Auto,	https://www. qualcomm.co m/company/ product- security/bull	O-QUA-APQ8- 200921/2418
CVSS Scoring Sc	ale 0-1	1-2	2-3 3-4 4-5 5-6	6-7 7-8	8-9 9-10

Page 968 of 1474

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Voice & Music, Snapdragon Wearables	etins/august- 2021-bulletin	
			CVE ID : CVE-2021-1916		
Integer Underflow (Wrap or Wraparoun d)	08-Sep-21	10	Integer underflow can occur when the RTCP length is lesser than than the actual blocks present in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Voice & Music, Snapdragon Wearables	https://www. qualcomm.co m/company/ product- security/bull etins/august- 2021-bulletin	O-QUA-APQ8- 200921/2419
			CVE ID : CVE-2021-1919		
Integer Underflow (Wrap or Wraparoun d)	08-Sep-21	10	Integer underflow can occur due to improper handling of incoming RTCP packets in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Voice & Music, Snapdragon Wearables	https://www. qualcomm.co m/company/ product- security/bull etins/august- 2021-bulletin	O-QUA-APQ8- 200921/2420
			CVE ID : CVE-2021-1920		
Exposure of Resource to Wrong Sphere	08-Sep-21	2.1	Lack of strict validation of bootmode can lead to information disclosure in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity,	https://www. qualcomm.co m/company/ product- security/bull etins/august-	O-QUA-APQ8- 200921/2421

0-1

1-2

5-6

6-7

7-8

8-9

Weakness	Publish Date	CVSS	Description & CVE I	Patch		NCII	PC ID	
			Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wearables		2021-bi	ulletin		
			CVE ID : CVE-2021-19					
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	08-Sep-21	10	Possible buffer overflor to improper validation device types during P2 search in Snapdragon A Snapdragon Compute, Snapdragon Connective Snapdragon Consumer Snapdragon Industrial Snapdragon Mobile, Snapdragon Woice & Me Snapdragon Wearables Snapdragon Wired Infrastructure and Networking CVE ID : CVE-2021-19	https:// qualcom m/com product security etins/au 2021-bu	nm.co pany/ :- v/bull ugust-	-	-APQ8- 1/2422	
aqt1000_firm	aqt1000_firmware							
Exposure of Resource to Wrong Sphere	08-Sep-21	2.1	Child process can leak information from paren process due to numeric are getting compared a these pid can be reused Snapdragon Auto, Snapdragon Compute, Snapdragon Connective Snapdragon Consumer Snapdragon Industrial Snapdragon Mobile, Snapdragon Wearables CVE ID : CVE-2021-19	https://www. qualcomm.co m/company/ product- security/bull etins/august- 2021-bulletin		-	-AQT1- 1/2423	
Loop with Unreachable Exit	08-Sep-21	5	Loop with unreachable condition may occur du improper handling of	https://www. qualcomm.co m/company/			-AQT1- 1/2424	
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 & CVE ID	Patch	NCIIPC ID
Condition ('Infinite Loop')			unsupported input inproduct-Snapdragon Auto,security/buSnapdragon Compute,etins/auguSnapdragon Connectivity,2021-bulleSnapdragon Consumer IOT,Snapdragon Industrial IOT,Snapdragon IoT, SnapdragonVoice & Music, SnapdragonWearablesCVE ID : CVE-2021-1914		
Out-of- bounds Write	08-Sep-21	10	Possible buffer underflow due to lack of check for negative indices values when processing user provided input in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Industrial IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Voice & Music, Snapdragon Wearableshttps://www qualcomm.co 		0-QUA-AQT1- 200921/2425
Integer Underflow (Wrap or Wraparoun d)	08-Sep-21	10	Integer underflow can occur when the RTCP length is lesser than than the actual blocks present in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Voice & Music, Snapdragon Wearables CVE ID : CVE-2021-1919	https://www. qualcomm.co m/company/ product- security/bull etins/august- 2021-bulletin	0-QUA-AQT1- 200921/2426
Integer Underflow	08-Sep-21	10	Integer underflow can occur due to improper handling of	https://www. qualcomm.co	0-QUA-AQT1-
(Wrap or			incoming RTCP packets in	m/company/	200921/2427

CVSS Scoring Scale	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10
Dago 071 of 1474										

Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
		Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Voice & Music, Snapdragon Wearables CVE ID : CVE-2021-1920	product- security/bull etins/august- 2021-bulletin	
08-Sep-21	4.6	Incorrect pointer argument passed to trusted application TA could result in un- intended memory operations in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Industrial IOT CVE ID : CVE-2021-1923	https://www. qualcomm.co m/company/ product- security/bull etins/august- 2021-bulletin	O-QUA-AQT1- 200921/2428
08-Sep-21	2.1	Lack of strict validation of bootmode can lead to information disclosure in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wearables CVE ID : CVE-2021-1929	https://www. qualcomm.co m/company/ product- security/bull etins/august- 2021-bulletin	0-QUA-AQT1- 200921/2429
r on ns e of a 08-Sep-21 09 08-Sep-21 09 08-Sep-21 09 08-Sep-21 09 08-Sep-21 09 08-Sep-21 09 08-Sep-21 00 00 00 00 00 00 00 00 00 00 00 00 00		https://www. qualcomm.co m/company/ product- security/bull etins/august- 2021-bulletin	0-QUA-AQT1- 200921/2430	
	08-Sep-21	08-Sep-21 4.6 08-Sep-21 2.1	Image: state in the state in	08-Sep-21Napdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Voice & Music, Snapdragon Nearablesproduct- security/bull etins/august- 2021-bulletin08-Sep-214.6Incorrect pointer argument passed to trusted application In Snapdragon Compute, Snapdragon Compute, Snapdragon Compute, Snapdragon Industrial IOT Snapdragon Connectivity, Snapdragon Connectivity, Snapdragon Connectivity, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Consumer IOT, Snapdragon Music, Snapdragon Consumer IOT, Snapdragon Consumer IOT, Snapdragon Mobile, Snapdragon Mobile, Snapdragon Mobile, Snapdragon Mobile, Snapdragon Mobile, Snapdragon Mobile, Snapdragon Mobile, Snapdragon Consumer IOT, Snapdragon Mobile, Snapdragon Mobile, Snapdragon Mobile, Snapdragon Mobile, Snapdragon Consumer IOT, Snapdragon Consumer IOT, Snapdragon Mobile, Snapdragon Mobile, Snapdragon Consumer IOT, Snapdragon Consumer IOT,

Weakness	Publish Date	CVSS	Description & CVE ID	Description & CVE ID Patch	
			CVE ID : CVE-2021-1930		
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	08-Sep-21	10	Possible buffer overflow due to improper validation of device types during P2P search in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Woice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking	https://www. qualcomm.co m/company/ product- security/bull etins/august- 2021-bulletin	0-QUA-AQT1- 200921/2431
			CVE ID : CVE-2021-1972		
ar6003_firm	ware				
Out-of- bounds Write	08-Sep-21	10	Possible buffer underflow due to lack of check for negative indices values when processing user provided input in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Voice & Music, Snapdragon Wearables CVE ID : CVE-2021-1916	https://www. qualcomm.co m/company/ product- security/bull etins/august- 2021-bulletin	0-QUA-AR60- 200921/2432
Integer Underflow (Wrap or Wraparoun d)	08-Sep-21	10	Integer underflow can occur due to improper handling of incoming RTCP packets in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT,	https://www. qualcomm.co m/company/ product- security/bull etins/august- 2021-bulletin	O-QUA-AR60- 200921/2433

0-1

1-2

7-8

5-6

6-7

8-9

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Snapdragon IoT, Snapdragon Voice & Music, Snapdragon Wearables		
			CVE ID : CVE-2021-1920		
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	08-Sep-21	10	Possible buffer overflow due to improper validation of device types during P2P search in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Woice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking CVE ID : CVE-2021-1972	https://www. qualcomm.co m/company/ product- security/bull etins/august- 2021-bulletin	0-QUA-AR60- 200921/2434
ar7420_firm	ware				
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	08-Sep-21	10	Possible buffer overflow due to improper validation of device types during P2P search in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Industrial IOT, Snapdragon Woice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking CVE ID : CVE-2021-1972	https://www. qualcomm.co m/company/ product- security/bull etins/august- 2021-bulletin	0-QUA-AR74- 200921/2435
ar8031_firm	ware				
Exposure of Resource to	08-Sep-21	2.1	Child process can leak information from parent	https://www. qualcomm.co	O-QUA-AR80-
CVSS Scoring Sc	ale 0-1	1-2	2-3 3-4 4-5 5-6 Page 974 of 1474	6-7 7-8	8-9 9-10

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Wrong Sphere			process due to numeric pids are getting compared and these pid can be reused in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wearables CVE ID : CVE-2021-1904	m/company/ product- security/bull etins/august- 2021-bulletin	200921/2436
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	08-Sep-21	10	Possible buffer overflow due to improper validation of device types during P2P search in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Industrial IOT, Snapdragon Woice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking CVE ID : CVE-2021-1972	https://www. qualcomm.co m/company/ product- security/bull etins/august- 2021-bulletin	0-QUA-AR80- 200921/2437
ar8035_firm	ware				
Exposure of Resource to Wrong Sphere	08-Sep-21	2.1	Child process can leak information from parent process due to numeric pids are getting compared and these pid can be reused in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile,	https://www. qualcomm.co m/company/ product- security/bull etins/august- 2021-bulletin	0-QUA-AR80- 200921/2438
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 & CVE ID	Patch	NCIIPC ID	
			Snapdragon Voice & Music, Snapdragon Wearables CVE ID : CVE-2021-1904			
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	08-Sep-21	10	Possible buffer overflow due to improper validation of device types during P2P search in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Woice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking CVE ID : CVE-2021-1972	https://www. qualcomm.co m/company/ product- security/bull etins/august- 2021-bulletin	O-QUA-AR80- 200921/2439	
ar9380_firm	ware					
Out-of- bounds Read	08-Sep-21	3.6	Buffer over read could occur due to incorrect check of buffer size while flashing emmc devices in Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking CVE ID : CVE-2021-1928	https://www. qualcomm.co m/company/ product- security/bull etins/august- 2021-bulletin	0-QUA-AR93- 200921/2440	
Buffer Copy without			Possible buffer overflow due to improper validation of	https://www. qualcomm.co		
Checking Size of Input ('Classic Buffer	08-Sep-21	10	device types during P2P search in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity,	qualcomm.co m/company/ product- security/bull etins/august-	0-QUA-AR93- 200921/2441	
CVSS Scoring Sc	ale 0-1	1-2	2-3 3-4 4-5 5-6	6-7 7-8	8-9 9-10	

Page 976 of 1474

Overflow') Overflow')Image: Second s	Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Exposure of Resource to Wrong Sphere08-Sep-212.1Child process can leak information from parent process due to numeric pids are getting compared and these pid can be reused in Snapdragon Compute, Snapdragon Consumer IOT, Snapdragon Consumer IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Voice & Music, Snapdragon Voice & Music, Snapdragon Consumer IOT, Snapdragon Voice & Music, Snapdragon Consumer IOT, Snapdragon Voice & Music, Snapdragon Voice & Music, Snapdragon Consumer IOT, Snapdragon Voice & Music, Snapdragon Consumer IOT, Snapdragon Voice & Music, Snapdragon Voice & Music, Snapdragon Consumer IOT, Snapdragon Consumer IOT, Snapdragon Voice & Music, Snapdragon Voice & Music, Snapdragon Voice & Music, Snapdragon Consumer IOT, Snapdragon Industrial IOT, <td>Overflow')</td> <td></td> <td></td> <td>Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking</td> <td>2021-bulletin</td> <td></td>	Overflow')			Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking	2021-bulletin	
Exposure of Resource to Wrong Sphere8.8Information from parent process due to numeric pids are getting compared and these pid can be reused in Snapdragon Compute, Snapdragon Consumer IOT, Snapdragon Muto, Snapdragon Consumer IOT, Snapdragon Mobile, Snapdragon Mobile, Snapdragon Wearableshttps://www. qualcomm.co m/company/ product- security/bull etins/august- 201-bulletin0-QUA-CSR6- 200921/2442Loop with Unreachable 	csr6030_firm	iware				
Loop with Unreachable Exit ConditionNapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Industrial IOT, Snapdragon Industrial IOT, Sonapdragon IoT, Snapdragon Voice & Music, Snapdragon Voice & ID : CVE-2021-1914O-QUA-CSR6- 200921/2443	Resource to Wrong	08-Sep-21	2.1	information from parent process due to numeric pids are getting compared and these pid can be reused in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wearables	qualcomm.co m/company/ product- security/bull etins/august-	=
Out-of- 08-Sep-21 10 Possible buffer underflow https://www. O-QUA-CSR6-	Unreachable Exit Condition ('Infinite	08-Sep-21	5	condition may occur due to improper handling of unsupported input in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Voice & Music, Snapdragon Wearables	qualcomm.co m/company/ product- security/bull etins/august-	•
	Out-of-	08-Sep-21	10	Possible buffer underflow	https://www.	0-QUA-CSR6-

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
bounds Write			due to lack of check for negative indices values when processing user provided input in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Voice & Music, Snapdragon Wearables	qualcomm.co m/company/ product- security/bull etins/august- 2021-bulletin	200921/2444
			CVE ID : CVE-2021-1916		
Integer Underflow (Wrap or Wraparoun d)	08-Sep-21	10	Integer underflow can occur when the RTCP length is lesser than than the actual blocks present in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Voice & Music, Snapdragon Wearables	https://www. qualcomm.co m/company/ product- security/bull etins/august- 2021-bulletin	0-QUA-CSR6- 200921/2445
			CVE ID : CVE-2021-1919		
Integer Underflow (Wrap or Wraparoun d)	08-Sep-21	10	Integer underflow can occur due to improper handling of incoming RTCP packets in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Voice & Music, Snapdragon Wearables	https://www. qualcomm.co m/company/ product- security/bull etins/august- 2021-bulletin	0-QUA-CSR6- 200921/2446
			CVE ID : CVE-2021-1920		0-QUA-CSR6-
Buffer Copy	08-Sep-21	10	Possible buffer overflow due to improper validation of	https://www. qualcomm.co	200921/2447

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Checking Size of Input ('Classic Buffer Overflow')			device types during P2P search in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Woice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking CVE ID : CVE-2021-1972	m/company/ product- security/bull etins/august- 2021-bulletin	
csr8811_firm	iware				
Out-of- bounds Read	08-Sep-21	3.6	Buffer over read could occur due to incorrect check of buffer size while flashing emmc devices in Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking CVE ID : CVE-2021-1928	https://www. qualcomm.co m/company/ product- security/bull etins/august- 2021-bulletin	0-QUA-CSR8- 200921/2448
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	08-Sep-21	10	Possible buffer overflow due to improper validation of device types during P2P search in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Woice & Music, Snapdragon Wearables, Snapdragon Wired	https://www. qualcomm.co m/company/ product- security/bull etins/august- 2021-bulletin	0-QUA-CSR8- 200921/2449

Page 979 of 1474

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Infrastructure and Networking		
			CVE ID : CVE-2021-1972		
			CVE ID : CVE-2021-1972		
csra6620_fir	mware				
Exposure of Resource to Wrong Sphere	08-Sep-21	2.1	Child process can leak information from parent process due to numeric pids are getting compared and these pid can be reused in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables	https://www. qualcomm.co m/company/ product- security/bull etins/august- 2021-bulletin	0-QUA-CSRA- 200921/2450
			CVE ID : CVE-2021-1904		
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	08-Sep-21	10	Possible buffer overflow due to improper validation of device types during P2P search in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Woice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking CVE ID : CVE-2021-1972	https://www. qualcomm.co m/company/ product- security/bull etins/august- 2021-bulletin	0-QUA-CSRA- 200921/2451
csra6640_fir	mware			<u> </u>	
Exposure of Resource to Wrong	08-Sep-21	2.1	Child process can leak information from parent process due to numeric pids are getting compared and	https://www. qualcomm.co m/company/ product-	0-QUA-CSRA- 200921/2452
CVSS Scoring Sc	ale 0-1	1-2	2-3 3-4 4-5 5-6 Page 980 of 1474	6-7 7-8	8-9 9-10

Page 980 of 1474

Weakness	Publish Date	CVSS	Description & CVE ID Patch		NCIIPC ID
Sphere			these pid can be reused in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables CVE ID : CVE-2021-1904	security/bull etins/august- 2021-bulletin	
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	08-Sep-21	10	Possible buffer overflow due to improper validation of device types during P2P search in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Industrial IOT, Snapdragon Woile, Snapdragon Woice & Music, Snapdragon Wired Infrastructure and Networking CVE ID : CVE-2021-1972	https://www. qualcomm.co m/company/ product- security/bull etins/august- 2021-bulletin	0-QUA-CSRA- 200921/2453
csrb31024_fi	irmware				
Exposure of Resource to Wrong Sphere	08-Sep-21	2.1	Child process can leak information from parent process due to numeric pids are getting compared and these pid can be reused in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music,	https://www. qualcomm.co m/company/ product- security/bull etins/august- 2021-bulletin	O-QUA-CSRB- 200921/2454

CVSS Scoring Scale	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10
			Pa	age 981 c	of 1474					

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Snapdragon Wearables		
			CVE ID : CVE-2021-1904		
Loop with Unreachable Exit Condition ('Infinite Loop')	08-Sep-21	5	Loop with unreachable exit condition may occur due to improper handling of unsupported input in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Voice & Music, Snapdragon Wearables	https://www. qualcomm.co m/company/ product- security/bull etins/august- 2021-bulletin	0-QUA-CSRB- 200921/2455
			CVE ID : CVE-2021-1914		
Out-of- bounds Write	08-Sep-21	10	Possible buffer underflow due to lack of check for negative indices values when processing user provided input in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Voice & Music, Snapdragon Wearables	https://www. qualcomm.co m/company/ product- security/bull etins/august- 2021-bulletin	0-QUA-CSRB- 200921/2456
			CVE ID : CVE-2021-1916		
Integer Underflow (Wrap or Wraparoun d)	08-Sep-21	10	Integer underflow can occur when the RTCP length is lesser than than the actual blocks present in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Voice & Music, Snapdragon	https://www. qualcomm.co m/company/ product- security/bull etins/august- 2021-bulletin	O-QUA-CSRB- 200921/2457

0-1

1-2

5-6

6-7

7-8

8-9

Integer Underflow	08-Sep-21		Wearables CVE ID : CVE-2021-1919 Integer underflow can occur due to improper handling of incoming RTCP packets in		
U	08-Sep-21		Integer underflow can occur due to improper handling of		
U	08-Sep-21		due to improper handling of		
(Wrap or 0 Wraparoun d)	r	10	Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Voice & Music, Snapdragon Wearables	https://www. qualcomm.co m/company/ product- security/bull etins/august- 2021-bulletin	0-QUA-CSRB- 200921/2458
			CVE ID : CVE-2021-1920		
Improper Restriction of Operations within the Bounds of a Memory Buffer	08-Sep-21	3.6	Possible out of bounds read due to incorrect validation of incoming buffer length in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile CVE ID : CVE-2021-1930	https://www. qualcomm.co m/company/ product- security/bull etins/august- 2021-bulletin	0-QUA-CSRB- 200921/2459
Buffer Copy without Checking Size of Input 0 ('Classic Buffer Overflow')	08-Sep-21	10	Possible buffer overflow due to improper validation of device types during P2P search in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Woice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking	https://www. qualcomm.co m/company/ product- security/bull etins/august- 2021-bulletin	0-QUA-CSRB- 200921/2460
CVSS Scoring Scale	e 0-1	1-2	2-3 3-4 4-5 5-6	6-7 7-8	8-9 9-10

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2021-1972		
fsm10055_fin	rmware				
Exposure of Resource to Wrong Sphere	08-Sep-21	2.1	Child process can leak information from parent process due to numeric pids are getting compared and these pid can be reused in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables	https://www. qualcomm.co m/company/ product- security/bull etins/august- 2021-bulletin	0-QUA-FSM1- 200921/2461
			CVE ID : CVE-2021-1904		
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	08-Sep-21	10	Possible buffer overflow due to improper validation of device types during P2P search in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Woice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking CVE ID : CVE-2021-1972	https://www. qualcomm.co m/company/ product- security/bull etins/august- 2021-bulletin	0-QUA-FSM1- 200921/2462
fsm10056_fii	rmware				L
Exposure of Resource to Wrong Sphere	08-Sep-21	2.1	Child process can leak information from parent process due to numeric pids are getting compared and these pid can be reused in Snapdragon Auto,	https://www. qualcomm.co m/company/ product- security/bull etins/august-	0-QUA-FSM1- 200921/2463
CVSS Scoring Sc	ale 0-1	1-2	2-3 3-4 4-5 5-6 Page 984 of 1474	6-7 7-8	8-9 9-10

Buffer Copy without (Classic Buffer Size of Input (Classic Buffer Size of Input (Classic Buffer Size of Input (Shapdragon Cansumer IOT, Snapdragon Mobile, Snapdragon Mobile, Snapdragon Wearables, Snapdragon Consumer IOT, Snapdragon Wearables, Snapdragon Wearables, Snapdragon Consumer IOT, Snapdragon Wearables, Snapdragon Consumer IOT, Snapdragon Mobile, Snapdragon Wearables, Snapdragon Consumer IOT, Snapdragon Mobile, Snapdragon Mobile, Snapdragon Mobile, Snapdragon Mobile, Snapdragon Mobile, Snapdragon Mobile, Snapdragon Mobile, Snapdragon Vice & Music, Snapdragon Wired Napdragon Wired Nearbles, Snapdragon Wired Networking CVE ID : CVE-2021-1972Poult-FSM1- 200921/2464 etins/august- 2021-bulletinOut-of- bounds Read08-Sep-213.6Buffer over read could occur due to incorrect check of buffer size while flashing emmc devices in Snapdragon Mobile, Snapdragon Connectivity, Snapdragon Mobile, Snap	Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')Ise and the search in Snapdragon Compute, Snapdragon Consumer IOT, Snapdragon Consumer IOT, Snapdragon Mobile, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wierd Infrastructure and Networkinghttps://www. qualcomm.co m/company/ product- security/bull etins/august- 2021-bulletinO-QUA-FSM1- 20921/2464Out-of- Dounds Read08-Sep-21and factor and the security of the security				Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables	2021-bulletin	
Out-of- bounds Read08-Sep-213.6Buffer over read could occur due to incorrect check of buffer size while flashing emmc devices in Snapdragon Connectivity, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Mosie, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networkinghttps://www. qualcomm.co m/company/ product- 	without Checking Size of Input ('Classic Buffer	08-Sep-21	10	to improper validation of device types during P2P search in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Woice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking	qualcomm.co m/company/ product- security/bull etins/august-	•
Out-of- bounds Read08-Sep-213.6due to incorrect check of buffer size while flashing emmc devices in Snapdragon Connectivity, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Mosic, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networkinghttps://www. qualcomm.co m/company/ product- security/bull etins/august- 2021-bulletin0-QUA-IPQ4- 200921/2465	ipq4018_firn	nware				
Buffer Copy 08-Sep-21 10 Possible buffer overflow due https://www. 0-QUA-IPQ4-	bounds	08-Sep-21	3.6	due to incorrect check of buffer size while flashing emmc devices in Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking	qualcomm.co m/company/ product- security/bull etins/august-	• •
	Buffer Copy	08-Sep-21	10	Possible buffer overflow due	https://www.	0-QUA-IPQ4-

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
without Checking Size of Input ('Classic Buffer Overflow')			to improper validation of device types during P2P search in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Woice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking	qualcomm.co m/company/ product- security/bull etins/august- 2021-bulletin	200921/2466
			CVE ID : CVE-2021-1972		
ipq4019_firm	iware				
Out-of- bounds Read	08-Sep-21	3.6	Buffer over read could occur due to incorrect check of buffer size while flashing emmc devices in Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking CVE ID : CVE-2021-1928	https://www. qualcomm.co m/company/ product- security/bull etins/august- 2021-bulletin	0-QUA-IPQ4- 200921/2467
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	08-Sep-21	10	Possible buffer overflow due to improper validation of device types during P2P search in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables,	https://www. qualcomm.co m/company/ product- security/bull etins/august- 2021-bulletin	0-QUA-IPQ4- 200921/2468

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Snapdragon Wired Infrastructure and Networking		
			CVE ID : CVE-2021-1972		
ipq4028_firm	nware				
Out-of- bounds Read	08-Sep-21	3.6	Buffer over read could occur due to incorrect check of buffer size while flashing emmc devices in Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking	https://www. qualcomm.co m/company/ product- security/bull etins/august- 2021-bulletin	0-QUA-IPQ4- 200921/2469
			CVE ID : CVE-2021-1928		
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	08-Sep-21	10	Possible buffer overflow due to improper validation of device types during P2P search in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Woice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking CVE ID : CVE-2021-1972	https://www. qualcomm.co m/company/ product- security/bull etins/august- 2021-bulletin	0-QUA-IPQ4- 200921/2470
ipq4029_firm	nware				
Out-of- bounds Read	08-Sep-21	3.6	Buffer over read could occur due to incorrect check of buffer size while flashing emmc devices in Snapdragon	https://www. qualcomm.co m/company/ product-	0-QUA-IPQ4- 200921/2471
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 & CVE ID	Patch	NCIIPC ID
			Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking CVE ID : CVE-2021-1928	security/bull etins/august- 2021-bulletin	
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	08-Sep-21	10	Possible buffer overflow due to improper validation of device types during P2P search in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Woice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking CVE ID : CVE-2021-1972	https://www. qualcomm.co m/company/ product- security/bull etins/august- 2021-bulletin	0-QUA-IPQ4- 200921/2472
ipq5010_firn	nware				
Out-of- bounds Read	08-Sep-21	3.6	Buffer over read could occur due to incorrect check of buffer size while flashing emmc devices in Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking CVE ID : CVE-2021-1928	https://www. qualcomm.co m/company/ product- security/bull etins/august- 2021-bulletin	O-QUA-IPQ5- 200921/2473
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 & CVE ID	Patch	NCIIPC ID
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	08-Sep-21	10	Possible buffer overflow due to improper validation of device types during P2P search in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Woice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking CVE ID : CVE-2021-1972	https://www. qualcomm.co m/company/ product- security/bull etins/august- 2021-bulletin	0-QUA-IPQ5- 200921/2474
ipq5018_firn	nware				
Out-of- bounds Read	08-Sep-21	3.6	Buffer over read could occur due to incorrect check of buffer size while flashing emmc devices in Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking CVE ID : CVE-2021-1928	https://www. qualcomm.co m/company/ product- security/bull etins/august- 2021-bulletin	0-QUA-IPQ5- 200921/2475
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	08-Sep-21	10	Possible buffer overflow due to improper validation of device types during P2P search in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music,	https://www. qualcomm.co m/company/ product- security/bull etins/august- 2021-bulletin	0-QUA-IPQ5- 200921/2476

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking		
			CVE ID : CVE-2021-1972		
ipq5028_firm	nware				
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	08-Sep-21	10	Possible buffer overflow due to improper validation of device types during P2P search in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Woice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking CVE ID : CVE-2021-1972	https://www. qualcomm.co m/company/ product- security/bull etins/august- 2021-bulletin	0-QUA-IPQ5- 200921/2477
ipq6000_firm	nware				
Out-of- bounds Read	08-Sep-21	3.6	Buffer over read could occur due to incorrect check of buffer size while flashing emmc devices in Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking CVE ID : CVE-2021-1928	https://www. qualcomm.co m/company/ product- security/bull etins/august- 2021-bulletin	O-QUA-IPQ6- 200921/2478
Buffer Copy without Checking	08-Sep-21 ale 0-1	10	Possible buffer overflow due to improper validation of device types during P2P 2-3 3-4 4-5 5-6	https://www. qualcomm.co m/company/	0-QUA-IPQ6- 200921/2479 8-9 9-10

		CVSS	Description & CVE ID	Patch	NCIIPC ID
Size of Input ('Classic Buffer Overflow')			search in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking CVE ID : CVE-2021-1972	product- security/bull etins/august- 2021-bulletin	
ipq6005_firm	iware				
Out-of- bounds Read	08-Sep-21	3.6	Buffer over read could occur due to incorrect check of buffer size while flashing emmc devices in Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking CVE ID : CVE-2021-1928	https://www. qualcomm.co m/company/ product- security/bull etins/august- 2021-bulletin	0-QUA-IPQ6- 200921/2480
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	08-Sep-21	10	Possible buffer overflow due to improper validation of device types during P2P search in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Woice & Music, Snapdragon Wired Infrastructure and	https://www. qualcomm.co m/company/ product- security/bull etins/august- 2021-bulletin	0-QUA-IPQ6- 200921/2481

Page 991 of 1474

Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
		Networking		
		CVE ID : CVE-2021-1972		
iware				
08-Sep-21	3.6	Buffer over read could occur due to incorrect check of buffer size while flashing emmc devices in Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking CVE ID : CVE-2021-1928	https://www. qualcomm.co m/company/ product- security/bull etins/august- 2021-bulletin	0-QUA-IPQ6- 200921/2482
08-Sep-21	10	Possible buffer overflow due to improper validation of device types during P2P search in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Woice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking CVE ID : CVE-2021-1972	https://www. qualcomm.co m/company/ product- security/bull etins/august- 2021-bulletin	0-QUA-IPQ6- 200921/2483
iware				
08-Sep-21	3.6	Buffer over read could occur due to incorrect check of buffer size while flashing emmc devices in Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon	https://www. qualcomm.co m/company/ product- security/bull etins/august-	0-QUA-IPQ6- 200921/2484
	1ware 08-Sep-21 08-Sep-21	Image: marked state sta	Image: state s	Networking CVE ID : CVE-2021-1972Networking CVE ID : CVE-2021-1972INVAREBuffer over read could occur due to incorrect check of buffer size while flashing emmc devices in Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Voice & Music, Snapdragon Voice & Music, Snapdragon Voice & Music, Snapdragon Verables, Snapdragon Verables, Snapdragon Noice & Music, Snapdragon Voice & Music, Snapdragon Networking CVE ID : CVE-2021-1928https://www. qualcomm.co m/company/ product- security/bull etins/august- 2021-bulletin08-Sep-2110Possible buffer overflow due to improper validation of device types during P2P search in Snapdragon Consumer IOT, Snapdragon Consumer IOT, Snapdragon Consumer IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Nobile, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking CVE ID : CVE-2021-1972https://www. qualcomm.co m/company/ product- security/bull etins/august- 2021-bulletin08-Sep-213.6Buffer over read could occur due to incorrect check of buffer size while flashing emmc devices in Snapdragon Connectivity, Snapdragon Connectivity, Snapdragon Connectivity, Snapdragon connectivity, Snapdragonhttps://www. qualcomm.co m/company/ product- security/bull etins/august- 2021-bulletin

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking	2021-bulletin	
			CVE ID : CVE-2021-1928		
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	08-Sep-21	10	Possible buffer overflow due to improper validation of device types during P2P search in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Woice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking CVE ID : CVE-2021-1972	https://www. qualcomm.co m/company/ product- security/bull etins/august- 2021-bulletin	0-QUA-IPQ6- 200921/2485
ipq6028_firm	nware				
Out-of- bounds Read	08-Sep-21	3.6	Buffer over read could occur due to incorrect check of buffer size while flashing emmc devices in Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking CVE ID : CVE-2021-1928	https://www. qualcomm.co m/company/ product- security/bull etins/august- 2021-bulletin	O-QUA-IPQ6- 200921/2486
Buffer Copy without	08-Sep-21	10	Possible buffer overflow due to improper validation of	https://www. qualcomm.co	0-QUA-IPQ6- 200921/2487

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Checking Size of Input ('Classic Buffer Overflow')			device types during P2P search in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Woice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking CVE ID : CVE-2021-1972	m/company/ product- security/bull etins/august- 2021-bulletin	
ipq8064_firn	nware				
Out-of- bounds Read	08-Sep-21	3.6	Buffer over read could occur due to incorrect check of buffer size while flashing emmc devices in Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking CVE ID : CVE-2021-1928	https://www. qualcomm.co m/company/ product- security/bull etins/august- 2021-bulletin	0-QUA-IPQ8- 200921/2488
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	08-Sep-21	10	Possible buffer overflow due to improper validation of device types during P2P search in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Woice & Music, Snapdragon Wearables, Snapdragon Wired	https://www. qualcomm.co m/company/ product- security/bull etins/august- 2021-bulletin	0-QUA-IPQ8- 200921/2489

Page 994 of 1474

ware		Infrastructure and Networking CVE ID : CVE-2021-1972					
ware		C					
ware		CVE ID : CVE-2021-1972					
ware							
08-Sep-21	3.6	Buffer over read could occur due to incorrect check of buffer size while flashing emmc devices in Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking CVE ID : CVE-2021-1928	https://www. qualcomm.co m/company/ product- security/bull etins/august- 2021-bulletin	0-QUA-IPQ8- 200921/2490			
08-Sep-21	10	Possible buffer overflow due to improper validation of device types during P2P search in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Woice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking CVE ID : CVE-2021-1972	https://www. qualcomm.co m/company/ product- security/bull etins/august- 2021-bulletin	0-QUA-IPQ8- 200921/2491			
pq8068_firmware							
08-Sep-21	3.6	Buffer over read could occur due to incorrect check of buffer size while flashing emmc devices in Snapdragon Connectivity, Snapdragon	https://www. qualcomm.co m/company/ product- security/bull	0-QUA-IPQ8- 200921/2492			
0	08-Sep-21 08-Sep-21	vare 08-Sep-21 10 vare 08-Sep-21 3.6	D8-Sep-213.6Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking08-Sep-21Possible buffer overflow due to improper validation of device types during P2P search in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Consumer IOT, Snapdragon Nobile, Snapdragon Wired Infrastructure and Networking08-Sep-2110Snapdragon Consumer IOT, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking08-Sep-213.6Buffer over read could occur due to incorrect check of buffer size while flashing emmc devices in Snapdragon connectivity, Snapdragon	D8-Sep-21Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networkingm/company/ product- security/bull etins/august- 2021-bulletinD8-Sep-21IPossible buffer overflow due to improper validation of device types during P2P search in Snapdragon Connectivity, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Consumer IOT, Snapdragon Mobile, Snapdragon Mobile, Snapdragon Mobile, Snapdragon Wired Infrastructure and Networking CVE ID : CVE-2021-1928https://www. qualcomm.co m/company/ product- security/bull etins/august- 2021-bulletinD8-Sep-21I0Snapdragon Industrial IOT, Snapdragon Wired Infrastructure and Networking CVE ID : CVE-2021-1972https://www. qualcomm.co m/company/ product- security/bull etins/august- 2021-bulletinD8-Sep-213.6Buffer over read could occur due to incorrect check of buffer size while flashing emmc devices in Snapdragon Councetivity, Snapdragon or duct- security/bull			

Buffer Copy without Checkingo.8-Sep-21I.0Suffer over read could occur dusic, Snapdragon Mobile, Snapdragon Compute, Snapdragon Nobile, Snapdragon Nobile, Snapdragon Voice & Music, Snapdragon Voice & Music, Snapdragon Voice & Music, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking CVE ID : CVE-2021-1972https://www. qualcomm.co m/company/ product- security/bull etins/august- 2021-bulletino-QUA-IPQ8- 200921/2493Out-of- bounds Read08-Sep-213.6Buffer over read could occur due to incorrect chek of buffer size while flashing emmc devices in Snapdragon Mobile, Snap	Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')Ise and the search in Snapdragon Compute, Snapdragon Consumer IOT, Snapdragon Consumer IOT, Snapdragon Mobile, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networkinghttps://www. qualcomm.co m/company/ product- security/bull etins/august- 2021-bulletino-QUA-IPQ8- 20921/2493Out-of- Dounds Read08-Sep-21Image Security Secu				Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking		
Out-of- bounds Read08-Sep-213.6Buffer over read could occur due to incorrect check of buffer size while flashing emmc devices in Snapdragon Connectivity, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wired Infrastructure and Networkinghttps://www. qualcomm.co m/company/ product- security/bull 	without Checking Size of Input ('Classic Buffer	08-Sep-21	10	to improper validation of device types during P2P search in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Woice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking	qualcomm.co m/company/ product- security/bull etins/august-	
Out-of- bounds Read08-Sep-213.6due to incorrect check of buffer size while flashing emmc devices in Snapdragon Connectivity, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Mosic, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networkinghttps://www. qualcomm.co m/company/ product- security/bull etins/august- 2021-bulletin0-QUA-IPQ8- 200921/2494	ipq8069_firn	nware				
Buffer Copy 08-Sep-21 10 Possible buffer overflow due https://www. 0-QUA-IPQ8-	bounds	08-Sep-21	3.6	due to incorrect check of buffer size while flashing emmc devices in Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking	qualcomm.co m/company/ product- security/bull etins/august-	
	Buffer Copy	08-Sep-21	10	Possible buffer overflow due	https://www.	0-QUA-IPQ8-

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
without Checking Size of Input ('Classic Buffer Overflow')			to improper validation of device types during P2P search in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Woice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking	qualcomm.co m/company/ product- security/bull etins/august- 2021-bulletin	200921/2495
i			CVE ID : CVE-2021-1972		
ipq8070a_fir	mware			Γ	1
Out-of- bounds Read	08-Sep-21	3.6	Buffer over read could occur due to incorrect check of buffer size while flashing emmc devices in Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking CVE ID : CVE-2021-1928	https://www. qualcomm.co m/company/ product- security/bull etins/august- 2021-bulletin	0-QUA-IPQ8- 200921/2496
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	08-Sep-21	10	Possible buffer overflow due to improper validation of device types during P2P search in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables,	https://www. qualcomm.co m/company/ product- security/bull etins/august- 2021-bulletin	0-QUA-IPQ8- 200921/2497

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Snapdragon Wired Infrastructure and Networking		
			CVE ID : CVE-2021-1972		
ipq8070_firn	nware				
Out-of- bounds Read	08-Sep-21	3.6	Buffer over read could occur due to incorrect check of buffer size while flashing emmc devices in Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking	https://www. qualcomm.co m/company/ product- security/bull etins/august- 2021-bulletin	0-QUA-IPQ8- 200921/2498
			CVE ID : CVE-2021-1928		
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	08-Sep-21	10	Possible buffer overflow due to improper validation of device types during P2P search in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Woice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking CVE ID : CVE-2021-1972	https://www. qualcomm.co m/company/ product- security/bull etins/august- 2021-bulletin	0-QUA-IPQ8- 200921/2499
ipq8071a_firmware					
Out-of- bounds Read	08-Sep-21	3.6	Buffer over read could occur due to incorrect check of buffer size while flashing emmc devices in Snapdragon	https://www. qualcomm.co m/company/ product-	0-QUA-IPQ8- 200921/2500
CVSS Scoring Sc	ale 0-1	1-2	2-3 3-4 4-5 5-6	6-7 7-8	8-9 <mark>9-10</mark>

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking CVE ID : CVE-2021-1928	security/bull etins/august- 2021-bulletin	
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	08-Sep-21	10	Possible buffer overflow due to improper validation of device types during P2P search in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Woice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking CVE ID : CVE-2021-1972	https://www. qualcomm.co m/company/ product- security/bull etins/august- 2021-bulletin	O-QUA-IPQ8- 200921/2501
ipq8071_firm	nware				
Out-of- bounds Read	08-Sep-21	3.6	Buffer over read could occur due to incorrect check of buffer size while flashing emmc devices in Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking CVE ID : CVE-2021-1928	https://www. qualcomm.co m/company/ product- security/bull etins/august- 2021-bulletin	0-QUA-IPQ8- 200921/2502
	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
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	08-Sep-21	10	Possible buffer overflow due to improper validation of device types during P2P search in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wired Infrastructure and Networking CVE ID : CVE-2021-1972	https://www. qualcomm.co m/company/ product- security/bull etins/august- 2021-bulletin	0-QUA-IPQ8- 200921/2503
ipq8072a_fir	mware				
Out-of- bounds Read	08-Sep-21	3.6	Buffer over read could occur due to incorrect check of buffer size while flashing emmc devices in Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking CVE ID : CVE-2021-1928	https://www. qualcomm.co m/company/ product- security/bull etins/august- 2021-bulletin	0-QUA-IPQ8- 200921/2504
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	08-Sep-21	10	Possible buffer overflow due to improper validation of device types during P2P search in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music,	https://www. qualcomm.co m/company/ product- security/bull etins/august- 2021-bulletin	0-QUA-IPQ8- 200921/2505

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking		
			CVE ID : CVE-2021-1972		
ipq8072_firm	iware				L
Out-of- bounds Read	08-Sep-21	3.6	Buffer over read could occur due to incorrect check of buffer size while flashing emmc devices in Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking CVE ID : CVE-2021-1928	https://www. qualcomm.co m/company/ product- security/bull etins/august- 2021-bulletin	0-QUA-IPQ8- 200921/2506
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	08-Sep-21	10	Possible buffer overflow due to improper validation of device types during P2P search in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Woice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking CVE ID : CVE-2021-1972	https://www. qualcomm.co m/company/ product- security/bull etins/august- 2021-bulletin	0-QUA-IPQ8- 200921/2507
ipq8074a_fir	mware				
Out-of- bounds	08-Sep-21	3.6	Buffer over read could occur due to incorrect check of buffer size while flashing	https://www. qualcomm.co m/company/	0-QUA-IPQ8- 200921/2508
CVSS Scoring Sc	ale 0-1	1-2	2-3 3-4 4-5 5-6 Page 1001 of 1474	6-7 7-8	8-9 9-10

Page 1001 of 1474

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Read			emmc devices in Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking CVE ID : CVE-2021-1928	product- security/bull etins/august- 2021-bulletin	
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	08-Sep-21	10	Possible buffer overflow due to improper validation of device types during P2P search in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Industrial IOT, Snapdragon Woice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking CVE ID : CVE-2021-1972	https://www. qualcomm.co m/company/ product- security/bull etins/august- 2021-bulletin	O-QUA-IPQ8- 200921/2509
ipq8074_firm	nware				
Out-of- bounds Read	08-Sep-21	3.6	Buffer over read could occur due to incorrect check of buffer size while flashing emmc devices in Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking	https://www. qualcomm.co m/company/ product- security/bull etins/august- 2021-bulletin	0-QUA-IPQ8- 200921/2510

CVSS Scoring Scale	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10
Page 1002 of 1474										

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2021-1928		
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	08-Sep-21	10	Possible buffer overflow due to improper validation of device types during P2P search in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Woice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking	https://www. qualcomm.co m/company/ product- security/bull etins/august- 2021-bulletin	0-QUA-IPQ8- 200921/2511
			CVE ID : CVE-2021-1972		
ipq8076a_fir	mware				
Out-of- bounds Read	08-Sep-21	3.6	Buffer over read could occur due to incorrect check of buffer size while flashing emmc devices in Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking CVE ID : CVE-2021-1928	https://www. qualcomm.co m/company/ product- security/bull etins/august- 2021-bulletin	0-QUA-IPQ8- 200921/2512
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	08-Sep-21	10	Possible buffer overflow due to improper validation of device types during P2P search in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT,	https://www. qualcomm.co m/company/ product- security/bull etins/august- 2021-bulletin	0-QUA-IPQ8- 200921/2513

1-2

0-1

5-6

6-7

7-8

8-9

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking CVE ID : CVE-2021-1972		
ipq8076_firn	nware				
Out-of- bounds Read	08-Sep-21	3.6	Buffer over read could occur due to incorrect check of buffer size while flashing emmc devices in Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking CVE ID : CVE-2021-1928	https://www. qualcomm.co m/company/ product- security/bull etins/august- 2021-bulletin	0-QUA-IPQ8- 200921/2514
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	08-Sep-21	10	Possible buffer overflow due to improper validation of device types during P2P search in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Woice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking CVE ID : CVE-2021-1972	https://www. qualcomm.co m/company/ product- security/bull etins/august- 2021-bulletin	0-QUA-IPQ8- 200921/2515
ipq8078a_fir	mware				

0-1

1-2

2-3 3-4 4-5

5-6

6-7

7-8

8-9

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Out-of- bounds Read	08-Sep-21	3.6	Buffer over read could occur due to incorrect check of buffer size while flashing emmc devices in Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking CVE ID : CVE-2021-1928	https://www. qualcomm.co m/company/ product- security/bull etins/august- 2021-bulletin	0-QUA-IPQ8- 200921/2516
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	08-Sep-21	10	Possible buffer overflow due to improper validation of device types during P2P search in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Woice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking CVE ID : CVE-2021-1972	https://www. qualcomm.co m/company/ product- security/bull etins/august- 2021-bulletin	O-QUA-IPQ8- 200921/2517
ipq8078_firn	nware				
Out-of- bounds Read	08-Sep-21	3.6	Buffer over read could occur due to incorrect check of buffer size while flashing emmc devices in Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon	https://www. qualcomm.co m/company/ product- security/bull etins/august- 2021-bulletin	0-QUA-IPQ8- 200921/2518

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Wired Infrastructure and		
			Networking		
			CVE ID : CVE-2021-1928		
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	08-Sep-21	10	Possible buffer overflow due to improper validation of device types during P2P search in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Industrial IOT, Snapdragon Woile, Snapdragon Woice & Music, Snapdragon Wired Infrastructure and Networking	https://www. qualcomm.co m/company/ product- security/bull etins/august- 2021-bulletin	0-QUA-IPQ8- 200921/2519
			CVE ID : CVE-2021-1972		
ipq8173_firm	nware				
Out-of- bounds Read	08-Sep-21	3.6	Buffer over read could occur due to incorrect check of buffer size while flashing emmc devices in Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking CVE ID : CVE-2021-1928	https://www. qualcomm.co m/company/ product- security/bull etins/august- 2021-bulletin	O-QUA-IPQ8- 200921/2520
Buffer Copy			Possible buffer overflow due	https://www.	
without Checking Size of Input ('Classic Buffer	08-Sep-21	10	to improper validation of device types during P2P search in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity,	qualcomm.co m/company/ product- security/bull etins/august-	0-QUA-IPQ8- 200921/2521
CVSS Scoring Sc	ale 0-1	1-2	2-3 3-4 4-5 5-6	6-7 7-8	8-9 9-10

Page 1006 of 1474

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Overflow')			Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking CVE ID : CVE-2021-1972	2021-bulletin	
ipq8174_firn	nware				
Out-of- bounds Read	08-Sep-21	3.6	Buffer over read could occur due to incorrect check of buffer size while flashing emmc devices in Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking	https://www. qualcomm.co m/company/ product- security/bull etins/august- 2021-bulletin	0-QUA-IPQ8- 200921/2522
			CVE ID : CVE-2021-1928		
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	08-Sep-21	10	Possible buffer overflow due to improper validation of device types during P2P search in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Woice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking CVE ID : CVE-2021-1972	https://www. qualcomm.co m/company/ product- security/bull etins/august- 2021-bulletin	0-QUA-IPQ8- 200921/2523

Page 1007 of 1474

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
mdm8207_fi	rmware				
Loop with Unreachable Exit Condition ('Infinite Loop')	08-Sep-21	5	Loop with unreachable exit condition may occur due to improper handling of unsupported input in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Voice & Music, Snapdragon Wearables CVE ID : CVE-2021-1914	https://www. qualcomm.co m/company/ product- security/bull etins/august- 2021-bulletin	O-QUA- MDM8- 200921/2524
Out-of- bounds Write	08-Sep-21	10	Possible buffer underflow due to lack of check for negative indices values when processing user provided input in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Voice & Music, Snapdragon Wearables CVE ID : CVE-2021-1916	https://www. qualcomm.co m/company/ product- security/bull etins/august- 2021-bulletin	O-QUA- MDM8- 200921/2525
Integer Underflow (Wrap or Wraparoun d)	08-Sep-21	10	Integer underflow can occur when the RTCP length is lesser than than the actual blocks present in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Voice & Music, Snapdragon Wearables	https://www. qualcomm.co m/company/ product- security/bull etins/august- 2021-bulletin	O-QUA- MDM8- 200921/2526

CVSS	Scoring	Scale	2
------	---------	-------	---

0-1

1-2

2-3 3-4

4-5

6-7

5-6

7-8

8-9

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2021-1919		
Integer Underflow (Wrap or Wraparoun d)	08-Sep-21	10	Integer underflow can occur due to improper handling of incoming RTCP packets in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Voice & Music, Snapdragon Wearables	https://www. qualcomm.co m/company/ product- security/bull etins/august- 2021-bulletin	O-QUA- MDM8- 200921/2527
mdm021Em	finmuono		CVE ID : CVE-2021-1920		
mdm8215m_	inimware				
Out-of- bounds Write	08-Sep-21	10	Possible buffer underflow due to lack of check for negative indices values when processing user provided input in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Voice & Music, Snapdragon Wearables CVE ID : CVE-2021-1916	https://www. qualcomm.co m/company/ product- security/bull etins/august- 2021-bulletin	O-QUA- MDM8- 200921/2528
Integer Underflow (Wrap or Wraparoun d)	08-Sep-21	10	Integer underflow can occur due to improper handling of incoming RTCP packets in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Voice & Music, Snapdragon Wearables	https://www. qualcomm.co m/company/ product- security/bull etins/august- 2021-bulletin	O-QUA- MDM8- 200921/2529
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 & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2021-1920		
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	08-Sep-21	10	Possible buffer overflow due to improper validation of device types during P2P search in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Woice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking	https://www. qualcomm.co m/company/ product- security/bull etins/august- 2021-bulletin	O-QUA- MDM8- 200921/2530
			CVE ID : CVE-2021-1972		
mdm8215_fi	rmware				
Out-of- bounds Write	08-Sep-21	10	Possible buffer underflow due to lack of check for negative indices values when processing user provided input in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Voice & Music, Snapdragon Wearables CVE ID : CVE-2021-1916	https://www. qualcomm.co m/company/ product- security/bull etins/august- 2021-bulletin	O-QUA- MDM8- 200921/2531
Integer Underflow (Wrap or Wraparoun d)	08-Sep-21	10	Integer underflow can occur due to improper handling of incoming RTCP packets in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT,	https://www. qualcomm.co m/company/ product- security/bull etins/august- 2021-bulletin	O-QUA- MDM8- 200921/2532

0-1

1-2

7-8

5-6

6-7

8-9

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Snapdragon IoT, Snapdragon Voice & Music, Snapdragon Wearables		
			CVE ID : CVE-2021-1920		
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	08-Sep-21	10	Possible buffer overflow due to improper validation of device types during P2P search in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Woice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking CVE ID : CVE-2021-1972	https://www. qualcomm.co m/company/ product- security/bull etins/august- 2021-bulletin	0-QUA- MDM8- 200921/2533
mdm8615m_	firmware				<u> </u>
Out-of- bounds Write	08-Sep-21	10	Possible buffer underflow due to lack of check for negative indices values when processing user provided input in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Voice & Music, Snapdragon Wearables CVE ID : CVE-2021-1916	https://www. qualcomm.co m/company/ product- security/bull etins/august- 2021-bulletin	0-QUA- MDM8- 200921/2534
Integer Underflow (Wrap or Wraparoun d)	08-Sep-21	10	Integer underflow can occur due to improper handling of incoming RTCP packets in Snapdragon Auto, Snapdragon Compute,	https://www. qualcomm.co m/company/ product- security/bull	O-QUA- MDM8- 200921/2535
Underflow (Wrap or Wraparoun		10	due to improper handling of incoming RTCP packets in Snapdragon Auto,	qualcomm.co m/company/ product-	MDM8-

Page 1011 of 1474

			Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Voice & Music, Snapdragon Wearables	etins/august- 2021-bulletin	
			CVE ID : CVE-2021-1920		
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	08-Sep-21	10	Possible buffer overflow due to improper validation of device types during P2P search in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Woice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking CVE ID : CVE-2021-1972	https://www. qualcomm.co m/company/ product- security/bull etins/august- 2021-bulletin	O-QUA- MDM8- 200921/2536
mdm9150_firn	nware				
Exposure of Resource to Wrong Sphere	08-Sep-21	2.1	Child process can leak information from parent process due to numeric pids are getting compared and these pid can be reused in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables CVE ID : CVE-2021-1904	https://www. qualcomm.co m/company/ product- security/bull etins/august- 2021-bulletin	0-QUA- MDM9- 200921/2537
Loop with 0	08-Sep-21	5	Loop with unreachable exit	https://www.	0-QUA-

Page 1012 of 1474

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Unreachable Exit Condition ('Infinite Loop')			condition may occur due to improper handling of unsupported input in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Voice & Music, Snapdragon Wearables CVE ID : CVE-2021-1914	qualcomm.co m/company/ product- security/bull etins/august- 2021-bulletin	MDM9- 200921/2538
			Possible buffer underflow		
Out-of- bounds Write	08-Sep-21	10	due to lack of check for negative indices values when processing user provided input in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Voice & Music, Snapdragon Wearables	https://www. qualcomm.co m/company/ product- security/bull etins/august- 2021-bulletin	0-QUA- MDM9- 200921/2539
			CVE ID : CVE-2021-1916		
Integer Underflow (Wrap or Wraparoun d)	08-Sep-21	10	Integer underflow can occur when the RTCP length is lesser than than the actual blocks present in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Voice & Music, Snapdragon Wearables	https://www. qualcomm.co m/company/ product- security/bull etins/august- 2021-bulletin	O-QUA- MDM9- 200921/2540
			CVE ID : CVE-2021-1919		
	08-Sep-21	10	Integer underflow can occur	https://www.	0-QUA-

 3-4
 4-5

 Page 1013 of 1474

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Underflow (Wrap or Wraparoun d)			due to improper handling of incoming RTCP packets in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Voice & Music, Snapdragon Wearables CVE ID : CVE-2021-1920	qualcomm.co m/company/ product- security/bull etins/august- 2021-bulletin	MDM9- 200921/2541
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	08-Sep-21	10	Possible buffer overflow due to improper validation of device types during P2P search in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Woice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking CVE ID : CVE-2021-1972	https://www. qualcomm.co m/company/ product- security/bull etins/august- 2021-bulletin	O-QUA- MDM9- 200921/2542
mdm9205_fi	rmware				
Loop with Unreachable Exit Condition ('Infinite Loop')	08-Sep-21	5	Loop with unreachable exit condition may occur due to improper handling of unsupported input in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Voice & Music, Snapdragon	https://www. qualcomm.co m/company/ product- security/bull etins/august- 2021-bulletin	O-QUA- MDM9- 200921/2543

CVSS Scoring Scale	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10
			Pa	age 1014 (of 1474					

		Wearables CVE ID : CVE-2021-1914 Possible buffer underflow		
		Possible buffer underflow		
08-Sep-21	10	due to lack of check for negative indices values when processing user provided input in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Voice & Music, Snapdragon Wearables	https://www. qualcomm.co m/company/ product- security/bull etins/august- 2021-bulletin	O-QUA- MDM9- 200921/2544
		CVE ID : CVE-2021-1916		
08-Sep-21	10	Integer underflow can occur due to improper handling of incoming RTCP packets in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Voice & Music, Snapdragon Wearables CVE ID : CVE-2021-1920	https://www. qualcomm.co m/company/ product- security/bull etins/august- 2021-bulletin	0-QUA- MDM9- 200921/2545
mware				
08-Sep-21	2.1	Child process can leak information from parent process due to numeric pids are getting compared and these pid can be reused in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT,	https://www. qualcomm.co m/company/ product- security/bull etins/august- 2021-bulletin	O-QUA- MDM9- 200921/2546
r (nware	nware	D8-Sep-21A 2.1Child process can leak information from parent process due to numeric pids are getting compared and these pid can be reused in Snapdragon Consumer IOT, Snapdragon IoT, Snapdragon Snapdragon Consumer IOT, Snapdragon Consumer IOT, Snapdragon Consumer IOT, Snapdragon Consumer IOT, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Voice & Music, Snapdragon Compute, Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer IOT, Snapdragon Consumer IOT, Snapdragon Consumer IOT, Snapdragon Industrial IOT	Napdragon Industrial IOT, Snapdragon IoT, Snapdragon Voice & Music, Snapdragon Wearablesetins/august- 2021-bulletinCVE ID : CVE-2021-1916Integer underflow can occur due to improper handling of incoming RTCP packets in Snapdragon Compute, Snapdragon Connectivity, Snapdragon Industrial IOT, Snapdragon Industrial IOT, Snapdragon Industrial IOT, Snapdragon Industrial IOT, Snapdragon Industrial IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Voice & Music, Snapdragon

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables CVE ID : CVE-2021-1904		
Loop with Unreachable Exit Condition ('Infinite Loop')	08-Sep-21	5	Loop with unreachable exit condition may occur due to improper handling of unsupported input in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Voice & Music, Snapdragon Wearables CVE ID : CVE-2021-1914	https://www. qualcomm.co m/company/ product- security/bull etins/august- 2021-bulletin	O-QUA- MDM9- 200921/2547
Out-of- bounds Write	08-Sep-21	10	Possible buffer underflow due to lack of check for negative indices values when processing user provided input in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Voice & Music, Snapdragon Wearables CVE ID : CVE-2021-1916	https://www. qualcomm.co m/company/ product- security/bull etins/august- 2021-bulletin	O-QUA- MDM9- 200921/2548
Integer Underflow (Wrap or Wraparoun d)	08-Sep-21	10	Integer underflow can occur when the RTCP length is lesser than than the actual blocks present in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT,	https://www. qualcomm.co m/company/ product- security/bull etins/august- 2021-bulletin	O-QUA- MDM9- 200921/2549

1-2

0-1

5-6

6-7

7-8

8-9

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Snapdragon IoT, Snapdragon Voice & Music, Snapdragon Wearables		
			CVE ID : CVE-2021-1919		
Integer Underflow (Wrap or Wraparoun d)	08-Sep-21	10	Integer underflow can occur due to improper handling of incoming RTCP packets in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Voice & Music, Snapdragon Wearables CVE ID : CVE-2021-1920	https://www. qualcomm.co m/company/ product- security/bull etins/august- 2021-bulletin	O-QUA- MDM9- 200921/2550
Out-of- bounds Read	08-Sep-21	3.6	Buffer over read could occur due to incorrect check of buffer size while flashing emmc devices in Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking CVE ID : CVE-2021-1928	https://www. qualcomm.co m/company/ product- security/bull etins/august- 2021-bulletin	O-QUA- MDM9- 200921/2551
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	08-Sep-21	10	Possible buffer overflow due to improper validation of device types during P2P search in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile,	https://www. qualcomm.co m/company/ product- security/bull etins/august- 2021-bulletin	O-QUA- MDM9- 200921/2552

1-2

0-1

5-6

6-7

7-8

8-9

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking		
mdm0207 fi			CVE ID : CVE-2021-1972		
mdm9207_fi	rmware		Loop with uproachable ovit		[
Loop with Unreachable Exit Condition ('Infinite Loop')	08-Sep-21	5	Loop with unreachable exit condition may occur due to improper handling of unsupported input in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Voice & Music, Snapdragon Wearables CVE ID : CVE-2021-1914	https://www. qualcomm.co m/company/ product- security/bull etins/august- 2021-bulletin	O-QUA- MDM9- 200921/2553
Out-of- bounds Write	08-Sep-21	10	Possible buffer underflow due to lack of check for negative indices values when processing user provided input in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Voice & Music, Snapdragon Wearables CVE ID : CVE-2021-1916	https://www. qualcomm.co m/company/ product- security/bull etins/august- 2021-bulletin	O-QUA- MDM9- 200921/2554
Integer Underflow (Wrap or Wraparoun d)	08-Sep-21	10	Integer underflow can occur when the RTCP length is lesser than than the actual blocks present in Snapdragon Auto, Snapdragon Compute,	https://www. qualcomm.co m/company/ product- security/bull	O-QUA- MDM9- 200921/2555
CVSS Scoring Sc	ale 0-1	1-2	2-3 3-4 4-5 5-6 Page 1018 of 1474	6-7 7-8	8-9 9-10

Page 1018 of 1474

d)anaptragon Industriar IOT, Snapdragon Voice & Music, Snapdragon Wearablesetins/august- 2021-bulletinmdm9215_firmwareCVE ID : CVE-2021-1920etins/august- 2021-bulletinmdm9215_firmwarePossible buffer underflow due to lack of check for negative indices values when processing user provided input in Snapdragon Compute, Snapdragon Compute, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Compute, Snapdragon Compute, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Industrial IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Wearables0-QUA- MDM9- 200921/2557Integer Underflow (Wrap or08-Sep-2110Integer underflow can occur due to improper handling of incoming RTCP packets inhttps://www. qualcomm.co m/company/ O-QUA- MDM9-	Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Integer Underflow (Wrap or U)08-Sep-21Integer uInteger underflow can occur due to improper handling of incoming RTCP packets in Snapdragon Compute, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Wearableshttps://www. qualcomm.co0-QUA- MDM9- 200921/2556mdm9215_inversePossible buffer underflow due to lack of check for negative indices values when processing user provided input in Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Industr				Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Voice & Music, Snapdragon		
Integer Underflow (Wrap or Wraparoun08-Sep-21Io<				CVE ID : CVE-2021-1919		
mdm9215_firmwareImage: constraint of the second	Underflow (Wrap or Wraparoun	08-Sep-21	10	due to improper handling of incoming RTCP packets in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Voice & Music, Snapdragon	qualcomm.co m/company/ product- security/bull etins/august-	
Out-of- bounds08-Sep-2110Possible buffer underflow due to lack of check for negative indices values when processing user provided input in Snapdragon Auto, Snapdragon Compute,https://www. qualcomm.co m/company/0-QUA- MDM9- 200921/2557Write08-Sep-2110Snapdragon Connectivity, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Voice & Music, Snapdragon Wearablesproduct- etins/august- 2021-bulletin0-QUA- MDM9- 200921/2557Integer Underflow (Wrap or Wraparoun08-Sep-2110Integer underflow can occur incoming RTCP packets in Snapdragon Auto,https://www. qualcomm.co m/company/ 200921/2558				CVE ID : CVE-2021-1920		
Out-of- bounds08-Sep-2110due to lack of check for negative indices values when processing user provided input in Snapdragon Auto, Snapdragon Conpute, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Industrial IOT, Snapdragon Industrial IOT, Voice & Music, Snapdragon Voice & Music, Snapdragon <b< td=""><td>mdm9215_fin</td><td>rmware</td><td></td><td></td><td></td><td></td></b<>	mdm9215_fin	rmware				
IntegerInteger underflow can occurhttps://www.Underflow08-Sep-2110Integer underflow can occurhttps://www.Wraparoun08-Sep-2110incoming RTCP packets in Snapdragon Auto,m/company/MDM9- 200921/2558	bounds	08-Sep-21	10	due to lack of check for negative indices values when processing user provided input in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Voice & Music, Snapdragon Wearables	qualcomm.co m/company/ product- security/bull etins/august-	-
	Underflow (Wrap or Wraparoun	08-Sep-21	10	Integer underflow can occur due to improper handling of incoming RTCP packets in Snapdragon Auto,	qualcomm.co m/company/ product-	-

Page 1019 of 1474

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Voice & Music, Snapdragon Wearables	etins/august- 2021-bulletin	
			CVE ID : CVE-2021-1920		
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	08-Sep-21	10	Possible buffer overflow due to improper validation of device types during P2P search in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Woice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking CVE ID : CVE-2021-1972	https://www. qualcomm.co m/company/ product- security/bull etins/august- 2021-bulletin	0-QUA- MDM9- 200921/2559
mdm9230_fi	rmware				
Out-of- bounds Write	08-Sep-21	10	Possible buffer underflow due to lack of check for negative indices values when processing user provided input in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Voice & Music, Snapdragon Wearables CVE ID : CVE-2021-1916	https://www. qualcomm.co m/company/ product- security/bull etins/august-	O-QUA- MDM9- 200921/2560
Integer Underflow	08-Sep-21	10	Integer underflow can occur due to improper handling of	https://www. qualcomm.co	O-QUA- MDM9-
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 & CVE ID	Patch	NCIIPC ID
(Wrap or Wraparoun d)			incoming RTCP packets in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Voice & Music, Snapdragon Wearables CVE ID : CVE-2021-1920	m/company/ product- security/bull etins/august- 2021-bulletin	200921/2561
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	08-Sep-21	10	Possible buffer overflow due to improper validation of device types during P2P search in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Woice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking CVE ID : CVE-2021-1972	https://www. qualcomm.co m/company/ product- security/bull etins/august- 2021-bulletin	O-QUA- MDM9- 200921/2562
mdm9250_fi	rmware				
Exposure of Resource to Wrong Sphere	08-Sep-21 2.1 Child process can leak information from parent process due to numeric pids are getting compared and these pid can be reused in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music,		https://www. qualcomm.co m/company/ product- security/bull etins/august- 2021-bulletin	O-QUA- MDM9- 200921/2563	

CVSS Scoring Scale	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10	
	Page 1021 of 1474										

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Snapdragon Wearables		
			CVE ID : CVE-2021-1904		
Loop with Unreachable Exit Condition ('Infinite Loop')	08-Sep-21	5	Loop with unreachable exit condition may occur due to improper handling of unsupported input in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Voice & Music, Snapdragon Wearables CVE ID : CVE-2021-1914	https://www. qualcomm.co m/company/ product- security/bull etins/august- 2021-bulletin	O-QUA- MDM9- 200921/2564
Out-of- bounds Write	08-Sep-21	10	Possible buffer underflow due to lack of check for negative indices values when processing user provided input in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Voice & Music, Snapdragon Wearables CVE ID : CVE-2021-1916	https://www. qualcomm.co m/company/ product- security/bull etins/august- 2021-bulletin	O-QUA- MDM9- 200921/2565
Integer Underflow (Wrap or Wraparoun d)	08-Sep-21	10	Integer underflow can occur when the RTCP length is lesser than than the actual blocks present in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Voice & Music, Snapdragon	https://www. qualcomm.co m/company/ product- security/bull etins/august- 2021-bulletin	O-QUA- MDM9- 200921/2566

0-1

1-2

2-3 3-4 4-5 Page 1022 of 1474 5-6

6-7

7-8

8-9

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Wearables		
			CVE ID : CVE-2021-1919		
Integer Underflow (Wrap or Wraparoun d)	08-Sep-21	10	Integer underflow can occur due to improper handling of incoming RTCP packets in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Voice & Music, Snapdragon Wearables	https://www. qualcomm.co m/company/ product- security/bull etins/august- 2021-bulletin	0-QUA- MDM9- 200921/2567
			CVE ID : CVE-2021-1920		
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	08-Sep-21	10	Possible buffer overflow due to improper validation of device types during P2P search in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Woice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking CVE ID : CVE-2021-1972	https://www. qualcomm.co m/company/ product- security/bull etins/august- 2021-bulletin	O-QUA- MDM9- 200921/2568
mdm9310_fi	rmware			I	
Out-of- bounds Write	08-Sep-21	10	Possible buffer underflow due to lack of check for negative indices values when processing user provided input in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT,	https://www. qualcomm.co m/company/ product- security/bull etins/august- 2021-bulletin	O-QUA- MDM9- 200921/2569
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 & CVE ID	Patch	NCIIPC ID
			Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Voice & Music, Snapdragon Wearables		
			CVE ID : CVE-2021-1916		
Integer Underflow (Wrap or Wraparoun d)	08-Sep-21	10	Integer underflow can occur due to improper handling of incoming RTCP packets in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Voice & Music, Snapdragon Wearables CVE ID : CVE-2021-1920	https://www. qualcomm.co m/company/ product- security/bull etins/august- 2021-bulletin	O-QUA- MDM9- 200921/2570
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	08-Sep-21	10	Possible buffer overflow due to improper validation of device types during P2P search in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Industrial IOT, Snapdragon Woile, Snapdragon Woice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking CVE ID : CVE-2021-1972	https://www. qualcomm.co m/company/ product- security/bull etins/august- 2021-bulletin	O-QUA- MDM9- 200921/2571
mdm9330_fi	rmware				
Out-of- bounds Write	08-Sep-21	10	Possible buffer underflow due to lack of check for negative indices values when processing user provided input in Snapdragon Auto,	https://www. qualcomm.co m/company/ product- security/bull	O-QUA- MDM9- 200921/2572
CVSS Scoring Sc	ale 0-1	1-2	2-3 3-4 4-5 5-6 Page 1024 of 1474	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 IoT, Snapdragon Voice & Music, Snapdragon Wearables CVE ID : CVE-2021-1916	etins/august- 2021-bulletin	
Integer Underflow (Wrap or Wraparoun d)	08-Sep-21	10	Integer underflow can occur due to improper handling of incoming RTCP packets in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Voice & Music, Snapdragon Wearables CVE ID : CVE-2021-1920	https://www. qualcomm.co m/company/ product- security/bull etins/august- 2021-bulletin	0-QUA- MDM9- 200921/2573
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	08-Sep-21	10	Possible buffer overflow due to improper validation of device types during P2P search in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Woice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking CVE ID : CVE-2021-1972	https://www. qualcomm.co m/company/ product- security/bull etins/august- 2021-bulletin	O-QUA- MDM9- 200921/2574
mdm9607_fi	rmware				
Exposure of Resource to	08-Sep-21	2.1	Child process can leak information from parent	https://www. qualcomm.co	O-QUA- MDM9-
CVSS Scoring Sc	ale 0-1	1-2	2-3 3-4 4-5 5-6 Page 1025 of 1474	6-7 7-8	8-9 9-10

Page 1025 of 1474

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Wrong Sphere			process due to numeric pids are getting compared and these pid can be reused in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wearables CVE ID : CVE-2021-1904	m/company/ product- security/bull etins/august- 2021-bulletin	200921/2575
Loop with Unreachable Exit Condition ('Infinite Loop')	08-Sep-21	5	Loop with unreachable exit condition may occur due to improper handling of unsupported input in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Voice & Music, Snapdragon Wearables CVE ID : CVE-2021-1914	https://www. qualcomm.co m/company/ product- security/bull etins/august- 2021-bulletin	0-QUA- MDM9- 200921/2576
Out-of- bounds Write	08-Sep-21	10	Possible buffer underflow due to lack of check for negative indices values when processing user provided input in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Voice & Music, Snapdragon Wearables CVE ID : CVE-2021-1916	https://www. qualcomm.co m/company/ product- security/bull etins/august- 2021-bulletin	O-QUA- MDM9- 200921/2577

CVSS Scoring Scale	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	
Page 1026 of 1474									

9-10

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Integer Underflow (Wrap or Wraparoun d)	08-Sep-21	10	Integer underflow can occur when the RTCP length is lesser than than the actual blocks present in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Voice & Music, Snapdragon Wearables CVE ID : CVE-2021-1919	https://www. qualcomm.co m/company/ product- security/bull etins/august- 2021-bulletin	O-QUA- MDM9- 200921/2578
Integer Underflow (Wrap or Wraparoun d)	08-Sep-21	10	Integer underflow can occur due to improper handling of incoming RTCP packets in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Voice & Music, Snapdragon Wearables CVE ID : CVE-2021-1920	https://www. qualcomm.co m/company/ product- security/bull etins/august- 2021-bulletin	O-QUA- MDM9- 200921/2579
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	08-Sep-21	10	Possible buffer overflow due to improper validation of device types during P2P search in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Woice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking	https://www. qualcomm.co m/company/ product- security/bull etins/august- 2021-bulletin	O-QUA- MDM9- 200921/2580

CVSS Scoring Scale	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10
Page 1027 of 1474										

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2021-1972		
mdm9615m	firmware			I	L
Out-of- bounds Write	08-Sep-21	10	Possible buffer underflow due to lack of check for negative indices values when processing user provided input in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Voice & Music, Snapdragon Wearables	https://www. qualcomm.co m/company/ product- security/bull etins/august- 2021-bulletin	0-QUA- MDM9- 200921/2581
			CVE ID : CVE-2021-1916		
Integer Underflow (Wrap or Wraparoun d)	08-Sep-21	10	Integer underflow can occur due to improper handling of incoming RTCP packets in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Voice & Music, Snapdragon Wearables	https://www. qualcomm.co m/company/ product- security/bull etins/august- 2021-bulletin	O-QUA- MDM9- 200921/2582
			CVE ID : CVE-2021-1920		
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	08-Sep-21	10	Possible buffer overflow due to improper validation of device types during P2P search in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables,	https://www. qualcomm.co m/company/ product- security/bull etins/august- 2021-bulletin	O-QUA- MDM9- 200921/2583

0-1

1-2

2-3 3-4 4-5 Page 1028 of 1474 7-8

5-6

6-7

8-9

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Snapdragon Wired Infrastructure and Networking		
			CVE ID : CVE-2021-1972		
mdm9615_fi	rmware				
Out-of- bounds Write	08-Sep-21	10	Possible buffer underflow due to lack of check for negative indices values when processing user provided input in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Voice & Music, Snapdragon Wearables	https://www. qualcomm.co m/company/ product- security/bull etins/august- 2021-bulletin	0-QUA- MDM9- 200921/2584
			CVE ID : CVE-2021-1916		
Integer Underflow (Wrap or Wraparoun d)	08-Sep-21	10	Integer underflow can occur due to improper handling of incoming RTCP packets in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Voice & Music, Snapdragon Wearables	https://www. qualcomm.co m/company/ product- security/bull etins/august- 2021-bulletin	O-QUA- MDM9- 200921/2585
			CVE ID : CVE-2021-1920		
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	08-Sep-21	10	Possible buffer overflow due to improper validation of device types during P2P search in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT,	https://www. qualcomm.co m/company/ product- security/bull etins/august- 2021-bulletin	O-QUA- MDM9- 200921/2586
CVSS Scoring Sc	ale 0-1	1-2	2-3 3-4 4-5 5-6	6-7 7-8	8-9 9-10
			Page 1029 of 1474		

Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
		Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking		
		CVE ID : CVE-2021-1972		
rmware			L	L
08-Sep-21	10	Possible buffer underflow due to lack of check for negative indices values when processing user provided input in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Voice & Music, Snapdragon Wearables CVE ID : CVE-2021-1916	https://www. qualcomm.co m/company/ product- security/bull etins/august- 2021-bulletin	O-QUA- MDM9- 200921/2587
08-Sep-21	10	Integer underflow can occur when the RTCP length is lesser than than the actual blocks present in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Voice & Music, Snapdragon Wearables CVE ID : CVE-2021-1919	https://www. qualcomm.co m/company/ product- security/bull etins/august- 2021-bulletin	O-QUA- MDM9- 200921/2588
08-Sep-21	10	Integer underflow can occur due to improper handling of incoming RTCP packets in Snapdragon Auto, Snapdragon Compute,	https://www. qualcomm.co m/company/ product- security/bull	O-QUA- MDM9- 200921/2589
	rmware 08-Sep-21 08-Sep-21	08-Sep-21 10 08-Sep-21 10	Image: Construct of the second seco	Image: construct of the second seco

Page 1030 of 1474

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Voice & Music, Snapdragon Wearables	etins/august- 2021-bulletin	
			CVE ID : CVE-2021-1920		
mdm9626_fi	rmware				
Exposure of Resource to Wrong Sphere	08-Sep-21	2.1	Child process can leak information from parent process due to numeric pids are getting compared and these pid can be reused in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables CVE ID : CVE-2021-1904	https://www. qualcomm.co m/company/ product- security/bull etins/august- 2021-bulletin	O-QUA- MDM9- 200921/2590
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	08-Sep-21	10	Possible buffer overflow due to improper validation of device types during P2P search in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Woice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking CVE ID : CVE-2021-1972	https://www. qualcomm.co m/company/ product- security/bull etins/august- 2021-bulletin	O-QUA- MDM9- 200921/2591
mdm9628_fi	rmware			1	
CVSS Scoring Sc	ale 0-1	1-2	2-3 3-4 4-5 5-6 Page 1031 of 1474	6-7 7-8	8-9 9-10

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Exposure of Resource to Wrong Sphere	08-Sep-21	2.1	Child process can leak information from parent process due to numeric pids are getting compared and these pid can be reused in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables CVE ID : CVE-2021-1904	https://www. qualcomm.co m/company/ product- security/bull etins/august- 2021-bulletin	O-QUA- MDM9- 200921/2592
Loop with Unreachable Exit Condition ('Infinite Loop')	08-Sep-21	5	Loop with unreachable exit condition may occur due to improper handling of unsupported input in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Voice & Music, Snapdragon Wearables CVE ID : CVE-2021-1914	https://www. qualcomm.co m/company/ product- security/bull etins/august- 2021-bulletin	0-QUA- MDM9- 200921/2593
Out-of- bounds Write	08-Sep-21	10	Possible buffer underflow due to lack of check for negative indices values when processing user provided input in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Voice & Music, Snapdragon Wearables	https://www. qualcomm.co m/company/ product- security/bull etins/august- 2021-bulletin	0-QUA- MDM9- 200921/2594
CVSS Scoring Sc	ale 0-1	1-2	2-3 3-4 4-5 5-6 Page 1032 of 1474	6-7 7-8	8-9 9-10

Page 1032 of 1474

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2021-1916		
Integer Underflow (Wrap or Wraparoun d)	08-Sep-21	10	Integer underflow can occur when the RTCP length is lesser than than the actual blocks present in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Voice & Music, Snapdragon Wearables CVE ID : CVE-2021-1919	https://www. qualcomm.co m/company/ product- security/bull etins/august- 2021-bulletin	0-QUA- MDM9- 200921/2595
Integer Underflow (Wrap or Wraparoun d)	08-Sep-21	10	Integer underflow can occur due to improper handling of incoming RTCP packets in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Voice & Music, Snapdragon Wearables CVE ID : CVE-2021-1920	https://www. qualcomm.co m/company/ product- security/bull etins/august- 2021-bulletin	0-QUA- MDM9- 200921/2596
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	08-Sep-21	10	Possible buffer overflow due to improper validation of device types during P2P search in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Woice & Music, Snapdragon Wired Infrastructure and	https://www. qualcomm.co m/company/ product- security/bull etins/august- 2021-bulletin	O-QUA- MDM9- 200921/2597

CVSS Scoring Scale	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10
			Pa	age 1033	of 1474					

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID			
			Networking					
			CVE ID : CVE-2021-1972					
mdm9630_fi	mdm9630_firmware							
Out-of- bounds Write	08-Sep-21	10	Possible buffer underflow due to lack of check for negative indices values when processing user provided input in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Voice & Music, Snapdragon Wearables	https://www. qualcomm.co m/company/ product- security/bull etins/august- 2021-bulletin	O-QUA- MDM9- 200921/2598			
			CVE ID : CVE-2021-1916					
Integer Underflow (Wrap or Wraparoun d)	08-Sep-21	10	Integer underflow can occur due to improper handling of incoming RTCP packets in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Voice & Music, Snapdragon Wearables CVE ID : CVE-2021-1920	https://www. qualcomm.co m/company/ product- security/bull etins/august- 2021-bulletin	0-QUA- MDM9- 200921/2599			
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	08-Sep-21	10	Possible buffer overflow due to improper validation of device types during P2P search in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music,	https://www. qualcomm.co m/company/ product- security/bull etins/august- 2021-bulletin	O-QUA- MDM9- 200921/2600			
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 & CVE ID	Patch	NCIIPC ID
			Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking		
			CVE ID : CVE-2021-1972		
mdm9635m_	firmware				
Out-of- bounds Write	08-Sep-21	10	Possible buffer underflow due to lack of check for negative indices values when processing user provided input in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Voice & Music, Snapdragon Wearables CVE ID : CVE-2021-1916	https://www. qualcomm.co m/company/ product- security/bull etins/august- 2021-bulletin	O-QUA- MDM9- 200921/2601
Integer Underflow (Wrap or Wraparoun d)	08-Sep-21	10	Integer underflow can occur when the RTCP length is lesser than than the actual blocks present in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Voice & Music, Snapdragon Wearables CVE ID : CVE-2021-1919	https://www. qualcomm.co m/company/ product- security/bull etins/august- 2021-bulletin	0-QUA- MDM9- 200921/2602
Integer Underflow (Wrap or Wraparoun d)	08-Sep-21	10	Integer underflow can occur due to improper handling of incoming RTCP packets in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT,	https://www. qualcomm.co m/company/ product- security/bull etins/august- 2021-bulletin	O-QUA- MDM9- 200921/2603

Page 1035 of 1474

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Voice & Music, Snapdragon Wearables		
			CVE ID : CVE-2021-1920		
mdm9640_fii	rmware				
Exposure of Resource to Wrong Sphere	08-Sep-21	2.1	Child process can leak information from parent process due to numeric pids are getting compared and these pid can be reused in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables CVE ID : CVE-2021-1904	https://www. qualcomm.co m/company/ product- security/bull etins/august- 2021-bulletin	O-QUA- MDM9- 200921/2604
Loop with Unreachable Exit Condition ('Infinite Loop')	08-Sep-21	5	Loop with unreachable exit condition may occur due to improper handling of unsupported input in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Voice & Music, Snapdragon Wearables CVE ID : CVE-2021-1914	https://www. qualcomm.co m/company/ product- security/bull etins/august- 2021-bulletin	O-QUA- MDM9- 200921/2605
Out-of- bounds Write	08-Sep-21	10	Possible buffer underflow due to lack of check for negative indices values when processing user provided input in Snapdragon Auto,	https://www. qualcomm.co m/company/ product- security/bull	O-QUA- MDM9- 200921/2606
CVSS Scoring Sc	ale 0-1	1-2	2-3 3-4 4-5 5-6	6-7 7-8	8-9 9-10

Page 1036 of 1474

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Voice & Music, Snapdragon Wearables	etins/august- 2021-bulletin	
			CVE ID : CVE-2021-1916		
Integer Underflow (Wrap or Wraparoun d)	08-Sep-21	10	Integer underflow can occur when the RTCP length is lesser than than the actual blocks present in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Voice & Music, Snapdragon Wearables	https://www. qualcomm.co m/company/ product- security/bull etins/august- 2021-bulletin	O-QUA- MDM9- 200921/2607
			CVE ID : CVE-2021-1919		
Integer Underflow (Wrap or Wraparoun d)	08-Sep-21	10	Integer underflow can occur due to improper handling of incoming RTCP packets in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Voice & Music, Snapdragon Wearables	https://www. qualcomm.co m/company/ product- security/bull etins/august- 2021-bulletin	O-QUA- MDM9- 200921/2608
			CVE ID : CVE-2021-1920		
Buffer Copy without Checking Size of Input ('Classic Buffer	08-Sep-21	10	Possible buffer overflow due to improper validation of device types during P2P search in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity,	https://www. qualcomm.co m/company/ product- security/bull etins/august-	O-QUA- MDM9- 200921/2609

0-1

1-2

2-3 3-4

4-5

5-6

6-7

7-8

8-9

	CVSS	Description & CVE ID	Patch	NCIIPC ID
		Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking CVE ID : CVE-2021-1972	2021-bulletin	
rmware			I	
08-Sep-21	10	Possible buffer underflow due to lack of check for negative indices values when processing user provided input in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Voice & Music, Snapdragon Wearables	https://www. qualcomm.co m/company/ product- security/bull etins/august- 2021-bulletin	O-QUA- MDM9- 200921/2610
08-Sep-21	10	CVE ID : CVE-2021-1916 Integer underflow can occur when the RTCP length is lesser than than the actual blocks present in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Voice & Music, Snapdragon Wearables CVE ID : CVE-2021-1919	https://www. qualcomm.co m/company/ product- security/bull etins/august- 2021-bulletin	O-QUA- MDM9- 200921/2611
08-Sep-21	10	Integer underflow can occur due to improper handling of incoming RTCP packets in	https://www. qualcomm.co m/company/	O-QUA- MDM9- 200921/2612
	08-Sep-21 08-Sep-21	08-Sep-21 10 08-Sep-21 10	Napdragon Industrial IOT, Snapdragon Noice & Music, Snapdragon Vice & Music, Snapdragon Wiearables, Snapdragon Wired Infrastructure and NetworkingTimearePossible buffer underflow due to lack of check for negative indices values when processing user provided input in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Connectivity, Snapdragon Industrial IOT, Snapdragon I	Napdragon Industrial I0T, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking CVE ID : CVE-2021-1972Tmware08-Sep-211010Snapdragon Connectivity, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Connectivity, Snapdragon Consumer I0T, Snapdragon Industrial I0T, Snapdragon Consumer I0T, Snapdragon Consumer I0T, Snapdragon Industrial I0T, Snapdragon Industrial I0T, Snapdragon Consumer I0T, Snapdragon Consumer I0T, Snapdragon Industrial I0T, Snapdragon Industrial I0T, Snapdragon Consumer I0T, Snapdragon Industrial I0T, Sna

Wraparoun (1)Image: Sinapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer I0T, Snapdragon Industrial I0T, Snapdragon Industrial I0T, Snapdragon Voice & Music, Snapdragon Voice & Music, Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer I0T, Snapdragon Noice & Music, Snapdragon Voice & Music, Snapdragon Nuch Snapdragon Consumer I0T, Snapdragon Nuch Snapdragon Nuch Snapdragon Nuch Snapdragon Connectivity, Snapdragon Nuch Snapdragon Connectivity, Snapdragon Nuch Snapdragon Nuch Snapdragon Connectivity, Snapdragon Connectivity, Snapdragon Nuch Snapdragon Connectivity, Snapdragon Consum	Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Exposure of Resource to Wrong Sphere08-Sep-212.1Child process can leak information from parent process due to numeric pids are getting compared and these pid can be reused in Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Compute, Snapdragon Compute, Snapdragon Compute, Snapdragon Auto, Snapdragon Auto, Snapdragon Consumer IOT, Snapdragon Industrial IOT, <b< td=""><td>-</td><td></td><td></td><td>Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Voice & Music, Snapdragon Wearables</td><td>security/bull etins/august-</td><td></td></b<>	-			Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Voice & Music, Snapdragon Wearables	security/bull etins/august-	
Exposure of Resource to Wrong Sphere08-Sep-212.1information from parent process due to numeric pids are getting compared and these pid can be reused in Snapdragon Auto, Snapdragon Connuctivity, Snapdragon Consumer IOT, Snapdragon Mobile, Snapdragon Wearableshttps://www. qualcomm.co m/company/ product- security/bull etins/august- 2021-bulletin0-QUA- MDM9- 200921/2613Loop with Unreachable Exit 	mdm9650_fi	rmware				
Loop with Unreachable Exit Conditioncondition may occur due to improper handling ofhttps://www. qualcomm.co08-Sep-215Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Voice & Music, Snapdragon Wearableshttps://www. qualcomm.co200921/2614	Resource to Wrong	08-Sep-21	2.1	information from parent process due to numeric pids are getting compared and these pid can be reused in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wearables	qualcomm.co m/company/ product- security/bull etins/august-	MDM9-
	Unreachable Exit Condition ('Infinite	08-Sep-21	5	condition may occur due to improper handling of unsupported input in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Voice & Music, Snapdragon Wearables	qualcomm.co m/company/ product- security/bull etins/august-	MDM9-
Out-of- 08-Sep-21 10 Possible buffer underflow https://www. O-QUA-	Out-of-	08-Sep-21	10	Possible buffer underflow	https://www.	0-QUA-

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
bounds Write			due to lack of check for negative indices values when processing user provided input in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Voice & Music, Snapdragon Wearables CVE ID : CVE-2021-1916	qualcomm.co m/company/ product- security/bull etins/august- 2021-bulletin	MDM9- 200921/2615
			Integer underflow can occur		
Integer Underflow (Wrap or Wraparoun d)	08-Sep-21	10	when the RTCP length is lesser than than the actual blocks present in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Voice & Music, Snapdragon Wearables	https://www. qualcomm.co m/company/ product- security/bull etins/august- 2021-bulletin	O-QUA- MDM9- 200921/2616
			CVE ID : CVE-2021-1919		
Integer Underflow (Wrap or Wraparoun d)	08-Sep-21	10	Integer underflow can occur due to improper handling of incoming RTCP packets in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Voice & Music, Snapdragon Wearables	https://www. qualcomm.co m/company/ product- security/bull etins/august- 2021-bulletin	O-QUA- MDM9- 200921/2617
			CVE ID : CVE-2021-1920		
Buffer Copy without	08-Sep-21	10	Possible buffer overflow due to improper validation of	https://www. qualcomm.co	O-QUA- MDM9-

CVSS Scoring Scale	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10
Dage 1040 of 1474										

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Checking Size of Input ('Classic Buffer Overflow')			device types during P2P search in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Woice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking CVE ID : CVE-2021-1972	m/company/ product- security/bull etins/august- 2021-bulletin	200921/2618
mdm9655_fi	rmware			L	
Out-of- bounds Write	08-Sep-21	10	Possible buffer underflow due to lack of check for negative indices values when processing user provided input in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Voice & Music, Snapdragon Wearables CVE ID : CVE-2021-1916	https://www. qualcomm.co m/company/ product- security/bull etins/august- 2021-bulletin	O-QUA- MDM9- 200921/2619
Integer Underflow (Wrap or Wraparoun d)	08-Sep-21	10	Integer underflow can occur when the RTCP length is lesser than than the actual blocks present in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Voice & Music, Snapdragon Wearables	https://www. qualcomm.co m/company/ product- security/bull etins/august- 2021-bulletin	O-QUA- MDM9- 200921/2620

CVSS Scoring Scale	0-1	1-2	2-3

4-5

6-7

5-6

7-8

8-9

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2021-1919		
Integer Underflow (Wrap or Wraparoun d)	08-Sep-21	10	Integer underflow can occur due to improper handling of incoming RTCP packets in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Voice & Music, Snapdragon Wearables CVE ID : CVE-2021-1920	https://www. qualcomm.co m/company/ product- security/bull etins/august- 2021-bulletin	O-QUA- MDM9- 200921/2621
msm8108_fi	rmware				
Loop with Unreachable Exit Condition ('Infinite Loop')	08-Sep-21	5	Loop with unreachable exit condition may occur due to improper handling of unsupported input in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Voice & Music, Snapdragon Wearables CVE ID : CVE-2021-1914	https://www. qualcomm.co m/company/ product- security/bull etins/august- 2021-bulletin	0-QUA- MSM8- 200921/2622
Out-of- bounds Write	08-Sep-21	10	Possible buffer underflow due to lack of check for negative indices values when processing user provided input in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Voice & Music, Snapdragon	https://www. qualcomm.co m/company/ product- security/bull etins/august- 2021-bulletin	0-QUA- MSM8- 200921/2623

CVSS Scoring Scale	0-1	1-2	2-3	3-4	4-5	5-6	
			Da	a 1017	of 1 1 7 1		

8-9

9-10

6-7

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Wearables		
			CVE ID : CVE-2021-1916		
Integer Underflow (Wrap or Wraparoun d)	rflow p or 08-Sep-21 10		Integer underflow can occur when the RTCP length is lesser than than the actual blocks present in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Voice & Music, Snapdragon Wearables	https://www. qualcomm.co m/company/ product- security/bull etins/august- 2021-bulletin	0-QUA- MSM8- 200921/2624
			CVE ID : CVE-2021-1919		
Integer Underflow (Wrap or Wraparoun d)	08-Sep-21	10	Integer underflow can occur due to improper handling of incoming RTCP packets in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Voice & Music, Snapdragon Wearables CVE ID : CVE-2021-1920	https://www. qualcomm.co m/company/ product- security/bull etins/august- 2021-bulletin	0-QUA- MSM8- 200921/2625
msm8208_fii	rmware				
Loop with Unreachable Exit Condition ('Infinite Loop')	08-Sep-21	5	Loop with unreachable exit condition may occur due to improper handling of unsupported input in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Voice & Music, Snapdragon	https://www. qualcomm.co m/company/ product- security/bull etins/august- 2021-bulletin	0-QUA- MSM8- 200921/2626
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 & CVE ID	Patch	NCIIPC ID
			Wearables		
			CVE ID : CVE-2021-1914		
Out-of- bounds Write	08-Sep-21	10	Possible buffer underflow due to lack of check for negative indices values when processing user provided input in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Voice & Music, Snapdragon Wearables	https://www. qualcomm.co m/company/ product- security/bull etins/august- 2021-bulletin	O-QUA- MSM8- 200921/2627
			CVE ID : CVE-2021-1916		
Integer Underflow (Wrap or Wraparoun d)	08-Sep-21	10	Integer underflow can occur when the RTCP length is lesser than than the actual blocks present in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Voice & Music, Snapdragon Wearables CVE ID : CVE-2021-1919	https://www. qualcomm.co m/company/ product- security/bull etins/august- 2021-bulletin	O-QUA- MSM8- 200921/2628
Integer Underflow (Wrap or Wraparoun d)	08-Sep-21	10	Integer underflow can occur due to improper handling of incoming RTCP packets in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Voice & Music, Snapdragon Wearables	https://www. qualcomm.co m/company/ product- security/bull etins/august- 2021-bulletin	O-QUA- MSM8- 200921/2629
CVSS Scoring Sc	ale 0-1	1-2	2-3 3-4 4-5 5-6	6-7 7-8	8-9 9-10

 3-4
 4-5

 Page 1044 of 1474

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2021-1920		
msm8209_fi	rmware				
Loop with Unreachable Exit Condition ('Infinite Loop')	08-Sep-21	5	Loop with unreachable exit condition may occur due to improper handling of unsupported input in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Voice & Music, Snapdragon Wearables CVE ID : CVE-2021-1914	https://www. qualcomm.co m/company/ product- security/bull etins/august- 2021-bulletin	0-QUA- MSM8- 200921/2630
Out-of- bounds Write	08-Sep-21	10	Possible buffer underflow due to lack of check for negative indices values when processing user provided input in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Voice & Music, Snapdragon Wearables CVE ID : CVE-2021-1916	https://www. qualcomm.co m/company/ product- security/bull etins/august- 2021-bulletin	0-QUA- MSM8- 200921/2631
			Integer underflow can occur		
Integer Underflow (Wrap or Wraparoun d)	08-Sep-21	10	when the RTCP length is lesser than than the actual blocks present in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Voice & Music, Snapdragon	https://www. qualcomm.co m/company/ product- security/bull etins/august- 2021-bulletin	0-QUA- MSM8- 200921/2632

0-1

1-2

2-3 3-4 4-5 Page 1045 of 1474 5-6

6-7

7-8

8-9

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Wearables CVE ID : CVE-2021-1919		
Integer Underflow (Wrap or Wraparoun d)	08-Sep-21	10	Integer underflow can occur due to improper handling of incoming RTCP packets in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Voice & Music, Snapdragon Wearables CVE ID : CVE-2021-1920	https://www. qualcomm.co m/company/ product- security/bull etins/august- 2021-bulletin	O-QUA- MSM8- 200921/2633
msm8608_fin	rmware				I
Loop with Unreachable Exit Condition ('Infinite Loop')	08-Sep-21	5	Loop with unreachable exit condition may occur due to improper handling of unsupported input in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Voice & Music, Snapdragon Wearables CVE ID : CVE-2021-1914	https://www. qualcomm.co m/company/ product- security/bull etins/august- 2021-bulletin	0-QUA- MSM8- 200921/2634
Out-of- bounds Write	08-Sep-21	10	Possible buffer underflow due to lack of check for negative indices values when processing user provided input in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon	https://www. qualcomm.co m/company/ product- security/bull etins/august- 2021-bulletin	O-QUA- MSM8- 200921/2635
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 & CVE ID	Patch	NCIIPC ID
			Voice & Music, Snapdragon Wearables CVE ID : CVE-2021-1916		
Integer Underflow (Wrap or Wraparoun d)	08-Sep-21	10	Integer underflow can occur when the RTCP length is lesser than than the actual blocks present in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Voice & Music, Snapdragon Wearables	the RTCP length is than than the actual present in Snapdragon Snapdragon Compute, ragon Connectivity, ragon Consumer IOT, ragon Industrial IOT, ragon IoT, Snapdragon & Music, Snapdragon	
			CVE ID : CVE-2021-1919		
Integer Underflow (Wrap or Wraparoun d)	08-Sep-21	10	Integer underflow can occur due to improper handling of incoming RTCP packets in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Voice & Music, Snapdragon Wearables CVE ID : CVE-2021-1920	https://www. qualcomm.co m/company/ product- security/bull etins/august- 2021-bulletin	O-QUA- MSM8- 200921/2637
msm8909w_1	firmware				
Exposure of Resource to Wrong Sphere	08-Sep-21	Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT,		https://www. qualcomm.co m/company/ product- security/bull etins/august- 2021-bulletin	0-QUA- MSM8- 200921/2638
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 & CVE ID	Patch	NCIIPC ID
			Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables CVE ID : CVE-2021-1904		
Loop with Unreachable Exit Condition ('Infinite Loop')	08-Sep-21	5	Loop with unreachable exit condition may occur due to improper handling of unsupported input in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Voice & Music, Snapdragon Wearables	https://www. qualcomm.co m/company/ product- security/bull etins/august- 2021-bulletin	O-QUA- MSM8- 200921/2639
Out-of- bounds Write	08-Sep-21	10	CVE ID : CVE-2021-1914 Possible buffer underflow due to lack of check for negative indices values when processing user provided input in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Voice & Music, Snapdragon Wearables CVE ID : CVE-2021-1916	https://www. qualcomm.co m/company/ product- security/bull etins/august- 2021-bulletin	O-QUA- MSM8- 200921/2640
Integer Underflow (Wrap or Wraparoun d)	08-Sep-21	10	Integer underflow can occur when the RTCP length is lesser than than the actual blocks present in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT,	https://www. qualcomm.co m/company/ product- security/bull etins/august- 2021-bulletin	O-QUA- MSM8- 200921/2641

0-1

1-2

3-4 2-3 Page 1048 of 1474

4-5

5-6

6-7

7-8

8-9

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Snapdragon IoT, Snapdragon Voice & Music, Snapdragon Wearables		
			CVE ID : CVE-2021-1919		
Integer Underflow (Wrap or Wraparoun d)	08-Sep-21	10	Integer underflow can occur due to improper handling of incoming RTCP packets in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Voice & Music, Snapdragon Wearables	https://www. qualcomm.co m/company/ product- security/bull etins/august- 2021-bulletin	0-QUA- MSM8- 200921/2642
			CVE ID : CVE-2021-1920		
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	08-Sep-21	10	Possible buffer overflow due to improper validation of device types during P2P search in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Woice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking CVE ID : CVE-2021-1972	https://www. qualcomm.co m/company/ product- security/bull etins/august- 2021-bulletin	0-QUA- MSM8- 200921/2643
msm8917_fir	mware				
Exposure of Resource to Wrong Sphere	08-Sep-21	2.1	Child process can leak information from parent process due to numeric pids are getting compared and these pid can be reused in Snapdragon Auto,	https://www. qualcomm.co m/company/ product- security/bull etins/august-	0-QUA- MSM8- 200921/2644
CVSS Scoring Sc	ale 0-1	1-2	2-3 3-4 4-5 5-6 Page 1049 of 1474	6-7 7-8	8-9 9-10

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables	2021-bulletin	
			CVE ID : CVE-2021-1904		
Loop with Unreachable Exit Condition ('Infinite Loop')	08-Sep-21	5	Loop with unreachable exit condition may occur due to improper handling of unsupported input in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Voice & Music, Snapdragon Wearables CVE ID : CVE-2021-1914	https://www. qualcomm.co m/company/ product- security/bull etins/august- 2021-bulletin	O-QUA- MSM8- 200921/2645
Out-of- bounds Write	08-Sep-21	10	Possible buffer underflow due to lack of check for negative indices values when processing user provided input in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Voice & Music, Snapdragon Wearables CVE ID : CVE-2021-1916	https://www. qualcomm.co m/company/ product- security/bull etins/august- 2021-bulletin	O-QUA- MSM8- 200921/2646
Integer Underflow (Wrap or Wraparoun	08-Sep-21	10	Integer underflow can occur when the RTCP length is lesser than than the actual blocks present in Snapdragon	https://www. qualcomm.co m/company/ product-	O-QUA- MSM8- 200921/2647

CVSS Scoring Scale	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10
Page 1050 of 1474										

Page 1050 of 1474

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
d)			Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Voice & Music, Snapdragon Wearables CVE ID : CVE-2021-1919	security/bull etins/august- 2021-bulletin	
Integer Underflow (Wrap or Wraparoun d)	08-Sep-21	10	Integer underflow can occur due to improper handling of incoming RTCP packets in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Voice & Music, Snapdragon Wearables CVE ID : CVE-2021-1920	https://www. qualcomm.co m/company/ product- security/bull etins/august- 2021-bulletin	0-QUA- MSM8- 200921/2648
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	08-Sep-21	10	Possible buffer overflow due to improper validation of device types during P2P search in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Woice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking CVE ID : CVE-2021-1972	https://www. qualcomm.co m/company/ product- security/bull etins/august- 2021-bulletin	0-QUA- MSM8- 200921/2649
msm8920_fir	mware				
Loop with Unreachable	08-Sep-21	5	Loop with unreachable exit condition may occur due to	https://www. qualcomm.co	O-QUA- MSM8-
CVSS Scoring Sc	ale 0-1	1-2	2-3 3-4 4-5 5-6 Page 1051 of 1474	6-7 7-8	8-9 9-10

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Exit Condition ('Infinite Loop')			improper handling of unsupported input in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Voice & Music, Snapdragon Wearables CVE ID : CVE-2021-1914	m/company/ product- security/bull etins/august- 2021-bulletin	200921/2650
Out-of- bounds Write	08-Sep-21	10	Possible buffer underflow due to lack of check for negative indices values when processing user provided input in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Voice & Music, Snapdragon Wearables CVE ID : CVE-2021-1916	https://www. qualcomm.co m/company/ product- security/bull etins/august- 2021-bulletin	O-QUA- MSM8- 200921/2651
Integer Underflow (Wrap or Wraparoun d)	08-Sep-21	10	CVEID: CVE-2021-1910Integer underflow can occur when the RTCP length is lesser than than the actual blocks present in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Voice & Music, Snapdragon Wearableshttps://www. qualcomm.co m/company/ product- security/bull etins/august- 2021-bulletinCVE ID: CVE-2021-1919Ket Provide Note Comparison		0-QUA- MSM8- 200921/2652
Integer Underflow	08-Sep-21	10	Integer underflow can occur due to improper handling of	https://www. qualcomm.co	O-QUA- MSM8-

CVSS Scoring Scale	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10
Page 1052 of 1474										

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
(Wrap or Wraparoun d)			incoming RTCP packets in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Voice & Music, Snapdragon Wearables CVE ID : CVE-2021-1920	m/company/ product- security/bull etins/august- 2021-bulletin	200921/2653
msm8937_fir	mware			I	I
Loop with Unreachable Exit Condition ('Infinite Loop')	08-Sep-21	5	Loop with unreachable exit condition may occur due to improper handling of unsupported input in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Voice & Music, Snapdragon Wearables CVE ID : CVE-2021-1914	https://www. qualcomm.co m/company/ product- security/bull etins/august- 2021-bulletin	0-QUA- MSM8- 200921/2654
Out-of- bounds Write	08-Sep-21	10	Possible buffer underflow due to lack of check for negative indices values when processing user provided input in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Voice & Music, Snapdragon Wearables CVE ID : CVE-2021-1916	https://www. qualcomm.co m/company/ product- security/bull etins/august- 2021-bulletin	0-QUA- MSM8- 200921/2655
Integer	08-Sep-21	10	Integer underflow can occur	https://www.	0-QUA-

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Underflow (Wrap or Wraparoun d)			when the RTCP length is lesser than than the actual blocks present in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Voice & Music, Snapdragon Wearables CVE ID : CVE-2021-1919	qualcomm.co m/company/ product- security/bull etins/august- 2021-bulletin	MSM8- 200921/2656
Integer Underflow (Wrap or Wraparoun d)	08-Sep-21	10	Integer underflow can occur due to improper handling of incoming RTCP packets in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Voice & Music, Snapdragon Wearables CVE ID : CVE-2021-1920	https://www. qualcomm.co m/company/ product- security/bull etins/august- 2021-bulletin	0-QUA- MSM8- 200921/2657
msm8940_fir	rmware				
Loop with Unreachable Exit Condition ('Infinite Loop')	08-Sep-21	5	Loop with unreachable exit condition may occur due to improper handling of unsupported input in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Voice & Music, Snapdragon Wearables CVE ID : CVE-2021-1914	https://www. qualcomm.co m/company/ product- security/bull etins/august- 2021-bulletin	0-QUA- MSM8- 200921/2658
Out-of-	08-Sep-21	10	Possible buffer underflow	https://www.	0-QUA-
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 & CVE ID	Patch	NCIIPC ID			
bounds Write			due to lack of check for negative indices values when processing user provided input in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Voice & Music, Snapdragon Wearables CVE ID : CVE-2021-1916	qualcomm.co m/company/ product- security/bull etins/august- 2021-bulletin	MSM8- 200921/2659			
Integer Underflow (Wrap or Wraparoun d)	08-Sep-21	10	Integer underflow can occur when the RTCP length is lesser than than the actual blocks present in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Voice & Music, Snapdragon Wearables CVE ID : CVE-2021-1919	https://www. qualcomm.co m/company/ product- security/bull etins/august- 2021-bulletin	0-QUA- MSM8- 200921/2660			
Integer Underflow (Wrap or Wraparoun d)	08-Sep-21	10	Integer underflow can occur due to improper handling of incoming RTCP packets in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Voice & Music, Snapdragon Wearables CVE ID : CVE-2021-1920	https://www. qualcomm.co m/company/ product- security/bull etins/august- 2021-bulletin	O-QUA- MSM8- 200921/2661			
msm8953_firmware								
	08-Sep-21	2.1	Child process can leak	https://www.	0-QUA-			

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Resource to Wrong Sphere			information from parent process due to numeric pids are getting compared and these pid can be reused in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wearables CVE ID : CVE-2021-1904	qualcomm.co m/company/ product- security/bull etins/august- 2021-bulletin	MSM8- 200921/2662
Loop with Unreachable Exit Condition ('Infinite Loop')	08-Sep-21	5	Loop with unreachable exit condition may occur due to improper handling of unsupported input in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Voice & Music, Snapdragon Wearables CVE ID : CVE-2021-1914	https://www. qualcomm.co m/company/ product- security/bull etins/august- 2021-bulletin	0-QUA- MSM8- 200921/2663
Out-of- bounds Write	08-Sep-21	10	Possible buffer underflow due to lack of check for negative indices values when processing user provided input in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Voice & Music, Snapdragon Wearables	https://www. qualcomm.co m/company/ product- security/bull etins/august- 2021-bulletin	0-QUA- MSM8- 200921/2664

(CVSS Scoring Scale	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10
				Pa	age 1056 (of 1474					

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2021-1916		
Integer Underflow (Wrap or Wraparoun d)	08-Sep-21	10	Integer underflow can occur when the RTCP length is lesser than than the actual blocks present in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Voice & Music, Snapdragon Wearables CVE ID : CVE-2021-1919	https://www. qualcomm.co m/company/ product- security/bull etins/august- 2021-bulletin	0-QUA- MSM8- 200921/2665
Integer Underflow (Wrap or Wraparoun d)	08-Sep-21	10	Integer underflow can occur due to improper handling of incoming RTCP packets in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Voice & Music, Snapdragon Wearables CVE ID : CVE-2021-1920	https://www. qualcomm.co m/company/ product- security/bull etins/august- 2021-bulletin	0-QUA- MSM8- 200921/2666
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	08-Sep-21	10	Possible buffer overflow due to improper validation of device types during P2P search in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Woice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and	https://www. qualcomm.co m/company/ product- security/bull etins/august- 2021-bulletin	0-QUA- MSM8- 200921/2667

[CVSS Scoring Scale	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10
L				Pa	ge 1057	of 1474					

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Networking		
			CVE ID : CVE-2021-1972		
msm8976sg_	firmware				
Loop with Unreachable Exit Condition ('Infinite Loop')	08-Sep-21	5	Loop with unreachable exit condition may occur due to improper handling of unsupported input in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Voice & Music, Snapdragon Wearables CVE ID : CVE-2021-1914	https://www. qualcomm.co m/company/ product- security/bull etins/august- 2021-bulletin	0-QUA- MSM8- 200921/2668
Out-of- bounds Write	08-Sep-21	10	Possible buffer underflow due to lack of check for negative indices values when processing user provided input in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Voice & Music, Snapdragon Wearables CVE ID : CVE-2021-1916	https://www. qualcomm.co m/company/ product- security/bull etins/august- 2021-bulletin	0-QUA- MSM8- 200921/2669
Integer Underflow (Wrap or Wraparoun d)	08-Sep-21	10	Integer underflow can occur when the RTCP length is lesser than than the actual blocks present in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon	https://www. qualcomm.co m/company/ product- security/bull etins/august- 2021-bulletin	O-QUA- MSM8- 200921/2670
CVSS Scoring Sc	ale 0-1	1-2	2-3 3-4 4-5 5-6	6-7 7-8	8-9 9-10

Page 1058 of 1474

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Voice & Music, Snapdragon Wearables CVE ID : CVE-2021-1919		
Integer Underflow (Wrap or Wraparoun d)	08-Sep-21	10	Integer underflow can occur due to improper handling of incoming RTCP packets in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Voice & Music, Snapdragon Wearables CVE ID : CVE-2021-1920	https://www. qualcomm.co m/company/ product- security/bull etins/august- 2021-bulletin	0-QUA- MSM8- 200921/2671
msm8976_fi	rmware				
Loop with Unreachable Exit Condition ('Infinite Loop')	08-Sep-21	5	Loop with unreachable exit condition may occur due to improper handling of unsupported input in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Voice & Music, Snapdragon Wearables CVE ID : CVE-2021-1914	https://www. qualcomm.co m/company/ product- security/bull etins/august- 2021-bulletin	O-QUA- MSM8- 200921/2672
Out-of- bounds Write	08-Sep-21	10	Possible buffer underflow due to lack of check for negative indices values when processing user provided input in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT,	https://www. qualcomm.co m/company/ product- security/bull etins/august- 2021-bulletin	O-QUA- MSM8- 200921/2673
CVSS Scoring Sc	ale 0-1	1-2	2-3 3-4 4-5 5-6	6-7 7-8	8-9 9-10

 3-4
 4-5

 Page 1059 of 1474

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Snapdragon IoT, Snapdragon Voice & Music, Snapdragon Wearables		
			CVE ID : CVE-2021-1916		
Integer Underflow (Wrap or Wraparoun d)	08-Sep-21	10	Integer underflow can occur when the RTCP length is lesser than than the actual blocks present in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Voice & Music, Snapdragon Wearables	https://www. qualcomm.co m/company/ product- security/bull etins/august- 2021-bulletin	O-QUA- MSM8- 200921/2674
			CVE ID : CVE-2021-1919		
Integer Underflow (Wrap or Wraparoun d)	08-Sep-21	10	Integer underflow can occur due to improper handling of incoming RTCP packets in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Voice & Music, Snapdragon Wearables	https://www. qualcomm.co m/company/ product- security/bull etins/august- 2021-bulletin	0-QUA- MSM8- 200921/2675
	C		CVE ID : CVE-2021-1920		
msm8996au Exposure of Resource to Wrong Sphere	_ firmware 08-Sep-21	2.1	Child process can leak information from parent process due to numeric pids are getting compared and these pid can be reused in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT,	https://www. qualcomm.co m/company/ product- security/bull etins/august- 2021-bulletin	O-QUA- MSM8- 200921/2676

Page 1060 of 1474

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables		
			CVE ID : CVE-2021-1904		
Loop with Unreachable Exit Condition ('Infinite Loop')	08-Sep-21	5	Loop with unreachable exit condition may occur due to improper handling of unsupported input in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Voice & Music, Snapdragon Wearables	https://www. qualcomm.co m/company/ product- security/bull etins/august- 2021-bulletin	O-QUA- MSM8- 200921/2677
			CVE ID : CVE-2021-1914		
Out-of- bounds Write	08-Sep-21	10	Possible buffer underflow due to lack of check for negative indices values when processing user provided input in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Voice & Music, Snapdragon Wearables CVE ID : CVE-2021-1916	https://www. qualcomm.co m/company/ product- security/bull etins/august- 2021-bulletin	O-QUA- MSM8- 200921/2678
Integer Underflow (Wrap or Wraparoun d)	08-Sep-21	10	Integer underflow can occur when the RTCP length is lesser than than the actual blocks present in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT,	https://www. qualcomm.co m/company/ product- security/bull etins/august- 2021-bulletin	O-QUA- MSM8- 200921/2679
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 & CVE ID	Patch	NCIIPC ID
			Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Voice & Music, Snapdragon Wearables		
			CVE ID : CVE-2021-1919		
Integer Underflow (Wrap or Wraparoun d)	08-Sep-21	10	Integer underflow can occur due to improper handling of incoming RTCP packets in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Voice & Music, Snapdragon Wearables	https://www. qualcomm.co m/company/ product- security/bull etins/august- 2021-bulletin	O-QUA- MSM8- 200921/2680
			CVE ID : CVE-2021-1920		
Exposure of Resource to Wrong Sphere	08-Sep-21	2.1	Lack of strict validation of bootmode can lead to information disclosure in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wearables	https://www. qualcomm.co m/company/ product- security/bull etins/august- 2021-bulletin	O-QUA- MSM8- 200921/2681
			CVE ID : CVE-2021-1929		
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	08-Sep-21	10	Possible buffer overflow due to improper validation of device types during P2P search in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music,	https://www. qualcomm.co m/company/ product- security/bull etins/august- 2021-bulletin	O-QUA- MSM8- 200921/2682

0-1

1-2 2-3 4-5

5-6

6-7

7-8

8-9

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking		
			CVE ID : CVE-2021-1972		
pmp8074_fir	mware			I	I
Out-of- bounds Read	08-Sep-21	3.6	Buffer over read could occur due to incorrect check of buffer size while flashing emmc devices in Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking CVE ID : CVE-2021-1928	https://www. qualcomm.co m/company/ product- security/bull etins/august- 2021-bulletin	0-QUA-PMP8- 200921/2683
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	08-Sep-21	10	Possible buffer overflow due to improper validation of device types during P2P search in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Woice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking CVE ID : CVE-2021-1972	https://www. qualcomm.co m/company/ product- security/bull etins/august- 2021-bulletin	0-QUA-PMP8- 200921/2684
qca1990_firm	nware				
Out-of- bounds	08-Sep-21	10	Possible buffer underflow due to lack of check for negative indices values when	https://www. qualcomm.co m/company/	0-QUA-QCA1- 200921/2685
CVSS Scoring Sc	cale 0-1	1-2	2-3 3-4 4-5 5-6 Page 1063 of 1474	6-7 7-8	8-9 9-10

Page 1063 of 1474

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Write			processing user provided input in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Voice & Music, Snapdragon Wearables CVE ID : CVE-2021-1916	product- security/bull etins/august- 2021-bulletin	
Integer Underflow (Wrap or Wraparoun d)	08-Sep-21	10	Integer underflow can occur due to improper handling of incoming RTCP packets in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Voice & Music, Snapdragon Wearables CVE ID : CVE-2021-1920	https://www. qualcomm.co m/company/ product- security/bull etins/august- 2021-bulletin	0-QUA-QCA1- 200921/2686
qca4004_firm	nware			I	L
Loop with Unreachable Exit Condition ('Infinite Loop')	08-Sep-21	5	Loop with unreachable exit condition may occur due to improper handling of unsupported input in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Voice & Music, Snapdragon Wearables CVE ID : CVE-2021-1914	https://www. qualcomm.co m/company/ product- security/bull etins/august- 2021-bulletin	0-QUA-QCA4- 200921/2687
Out-of- bounds	08-Sep-21	10	Possible buffer underflow due to lack of check for	https://www. qualcomm.co	0-QUA-QCA4- 200921/2688

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Write			negative indices values when processing user provided input in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Voice & Music, Snapdragon Wearables CVE ID : CVE-2021-1916	m/company/ product- security/bull etins/august- 2021-bulletin	
Integer Underflow (Wrap or Wraparoun d)	08-Sep-21	10	Integer underflow can occur due to improper handling of incoming RTCP packets in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Voice & Music, Snapdragon Wearables CVE ID : CVE-2021-1920	https://www. qualcomm.co m/company/ product- security/bull etins/august- 2021-bulletin	0-QUA-QCA4- 200921/2689
qca4020_firn	nware				
Exposure of Resource to Wrong Sphere	08-Sep-21	2.1	Child process can leak information from parent process due to numeric pids are getting compared and these pid can be reused in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wearables CVE ID : CVE-2021-1904	https://www. qualcomm.co m/company/ product- security/bull etins/august- 2021-bulletin	0-QUA-QCA4- 200921/2690
CVSS Scoring Sc	ale 0-1	1-2	2-3 3-4 4-5 5-6	6-7 7-8	8-9 9-10

 3-4
 4-5
 5-6
 6-7

 Page 1065 of 1474

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	08-Sep-21	10	Possible buffer overflow due to improper validation of device types during P2P search in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Woice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking CVE ID : CVE-2021-1972	https://www. qualcomm.co m/company/ product- security/bull etins/august- 2021-bulletin	0-QUA-QCA4- 200921/2691
qca4024_firm	nware				
Out-of- bounds Read	08-Sep-21	3.6	Buffer over read could occur due to incorrect check of buffer size while flashing emmc devices in Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking CVE ID : CVE-2021-1928	https://www. qualcomm.co m/company/ product- security/bull etins/august- 2021-bulletin	0-QUA-QCA4- 200921/2692
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	08-Sep-21	10	Possible buffer overflow due to improper validation of device types during P2P search in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music,	https://www. qualcomm.co m/company/ product- security/bull etins/august- 2021-bulletin	0-QUA-QCA4- 200921/2693

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking		
			CVE ID : CVE-2021-1972		
qca6174a_fir	mware				
Exposure of Resource to Wrong Sphere	08-Sep-21	2.1	Child process can leak information from parent process due to numeric pids are getting compared and these pid can be reused in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wearables CVE ID : CVE-2021-1904	https://www. qualcomm.co m/company/ product- security/bull etins/august- 2021-bulletin	0-QUA-QCA6- 200921/2694
Loop with Unreachable Exit Condition ('Infinite Loop')	08-Sep-21	5	Loop with unreachable exit condition may occur due to improper handling of unsupported input in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Voice & Music, Snapdragon Wearables CVE ID : CVE-2021-1914	https://www. qualcomm.co m/company/ product- security/bull etins/august- 2021-bulletin	O-QUA-QCA6- 200921/2695
Out-of- bounds Write	08-Sep-21	10	Possible buffer underflow due to lack of check for negative indices values when processing user provided input in Snapdragon Auto,	https://www. qualcomm.co m/company/ product- security/bull	0-QUA-QCA6- 200921/2696
CVSS Scoring Sc	ale 0-1	1-2	2-3 3-4 4-5 5-6	6-7 7-8	8-9 9-10

Page 1067 of 1474

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Voice & Music, Snapdragon Wearables	etins/august- 2021-bulletin	
			CVE ID : CVE-2021-1916		
Integer Underflow (Wrap or Wraparoun d)	08-Sep-21	10	Integer underflow can occur when the RTCP length is lesser than than the actual blocks present in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Voice & Music, Snapdragon Wearables CVE ID : CVE-2021-1919	https://www. qualcomm.co m/company/ product- security/bull etins/august- 2021-bulletin	0-QUA-QCA6- 200921/2697
Integer Underflow (Wrap or Wraparoun d)	08-Sep-21	10	Integer underflow can occur due to improper handling of incoming RTCP packets in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Voice & Music, Snapdragon Wearables CVE ID : CVE-2021-1920	https://www. qualcomm.co m/company/ product- security/bull etins/august- 2021-bulletin	0-QUA-QCA6- 200921/2698
Improper Restriction of Operations within the Bounds of a	08-Sep-21	3.6	Possible out of bounds read due to incorrect validation of incoming buffer length in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity,	https://www. qualcomm.co m/company/ product- security/bull etins/august-	0-QUA-QCA6- 200921/2699

1-2

0-1

5-6

6-7

7-8

8-9

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Memory Buffer			Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile CVE ID : CVE-2021-1930	2021-bulletin	
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	08-Sep-21	10	Possible buffer overflow due to improper validation of device types during P2P search in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Woice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking CVE ID : CVE-2021-1972	https://www. qualcomm.co m/company/ product- security/bull etins/august- 2021-bulletin	0-QUA-QCA6- 200921/2700
qca6174_firm	nware			I	L
Exposure of Resource to Wrong Sphere	08-Sep-21	2.1	Child process can leak information from parent process due to numeric pids are getting compared and these pid can be reused in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wearables CVE ID : CVE-2021-1904	https://www. qualcomm.co m/company/ product- security/bull etins/august- 2021-bulletin	0-QUA-QCA6- 200921/2701
Out-of- bounds Write	08-Sep-21	10	Possible buffer underflow due to lack of check for negative indices values when processing user provided	https://www. qualcomm.co m/company/ product-	0-QUA-QCA6- 200921/2702
CVSS Scoring Sc	ale 0-1	1-2	2-3 3-4 4-5 5-6	6-7 7-8	8-9 9-10

Page 1069 of 1474

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			input in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Voice & Music, Snapdragon Wearables	security/bull etins/august- 2021-bulletin	
Integer Underflow (Wrap or Wraparoun d)	08-Sep-21	10	CVE ID : CVE-2021-1916 Integer underflow can occur due to improper handling of incoming RTCP packets in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Voice & Music, Snapdragon Wearables CVE ID : CVE-2021-1920	https://www. qualcomm.co m/company/ product- security/bull etins/august- 2021-bulletin	0-QUA-QCA6- 200921/2703
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	08-Sep-21	10	Possible buffer overflow due to improper validation of device types during P2P search in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Industrial IOT, Snapdragon Woice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking CVE ID : CVE-2021-1972	https://www. qualcomm.co m/company/ product- security/bull etins/august- 2021-bulletin	0-QUA-QCA6- 200921/2704
	nware				L
qca6310_firm					

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Resource to Wrong Sphere			information from parent process due to numeric pids are getting compared and these pid can be reused in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wearables CVE ID : CVE-2021-1904	qualcomm.co m/company/ product- security/bull etins/august- 2021-bulletin	200921/2705
Loop with Unreachable Exit Condition ('Infinite Loop')	08-Sep-21	5	Loop with unreachable exit condition may occur due to improper handling of unsupported input in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Voice & Music, Snapdragon Wearables CVE ID : CVE-2021-1914	https://www. qualcomm.co m/company/ product- security/bull etins/august- 2021-bulletin	0-QUA-QCA6- 200921/2706
Out-of- bounds Write	08-Sep-21	10	Possible buffer underflow due to lack of check for negative indices values when processing user provided input in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Voice & Music, Snapdragon Wearables	https://www. qualcomm.co m/company/ product- security/bull etins/august- 2021-bulletin	0-QUA-QCA6- 200921/2707

CVSS Scoring Scale	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10
			Pa	age 1071	of 1474					

teger			CVE ID : CVE-2021-1916		
teger					
nderflow	08-Sep-21	10	Integer underflow can occur when the RTCP length is lesser than than the actual blocks present in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Voice & Music, Snapdragon Wearables CVE ID : CVE-2021-1919	https://www. qualcomm.co m/company/ product- security/bull etins/august- 2021-bulletin	0-QUA-QCA6- 200921/2708
teger nderflow Vrap or Traparoun	08-Sep-21	10	Integer underflow can occur due to improper handling of incoming RTCP packets in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Voice & Music, Snapdragon Wearables CVE ID : CVE-2021-1920	https://www. qualcomm.co m/company/ product- security/bull etins/august- 2021-bulletin	0-QUA-QCA6- 200921/2709
ut-of- ounds ead	08-Sep-21	3.6	Buffer over read could occur due to incorrect check of buffer size while flashing emmc devices in Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking CVE ID : CVE-2021-1928	https://www. qualcomm.co m/company/ product- security/bull etins/august- 2021-bulletin	O-QUA-QCA6- 200921/2710
CVSS Scoring Scal	ale 0-1	1-2	2-3 3-4 4-5 5-6	6-7 7-8	8-9 9-10

 3-4
 4-5
 5-6

 Page 1072 of 1474

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	08-Sep-21	10	Possible buffer overflow due to improper validation of device types during P2P search in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Woice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking CVE ID : CVE-2021-1972	https://www. qualcomm.co m/company/ product- security/bull etins/august- 2021-bulletin	0-QUA-QCA6- 200921/2711
qca6320_firm	nware				
Exposure of Resource to Wrong Sphere	08-Sep-21	2.1	Child process can leak information from parent process due to numeric pids are getting compared and these pid can be reused in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables CVE ID : CVE-2021-1904	https://www. qualcomm.co m/company/ product- security/bull etins/august- 2021-bulletin	0-QUA-QCA6- 200921/2712
Loop with Unreachable Exit Condition ('Infinite Loop')	08-Sep-21	5	Loop with unreachable exit condition may occur due to improper handling of unsupported input in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT,	https://www. qualcomm.co m/company/ product- security/bull etins/august- 2021-bulletin	0-QUA-QCA6- 200921/2713

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Snapdragon IoT, Snapdragon Voice & Music, Snapdragon Wearables		
			CVE ID : CVE-2021-1914		
Out-of- bounds Write	08-Sep-21	10	Possible buffer underflow due to lack of check for negative indices values when processing user provided input in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Voice & Music, Snapdragon Wearables	https://www. qualcomm.co m/company/ product- security/bull etins/august- 2021-bulletin	0-QUA-QCA6- 200921/2714
			CVE ID : CVE-2021-1916		
Integer Underflow (Wrap or Wraparoun d)	08-Sep-21	10	Integer underflow can occur when the RTCP length is lesser than than the actual blocks present in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Voice & Music, Snapdragon Wearables	https://www. qualcomm.co m/company/ product- security/bull etins/august- 2021-bulletin	O-QUA-QCA6- 200921/2715
			CVE ID : CVE-2021-1919		
Integer Underflow (Wrap or Wraparoun d)	08-Sep-21	10	Integer underflow can occur due to improper handling of incoming RTCP packets in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon	https://www. qualcomm.co m/company/ product- security/bull etins/august- 2021-bulletin	0-QUA-QCA6- 200921/2716

0-1

1-2

3-4 2-3 Page 1074 of 1474

4-5

6-7

5-6

7-8

8-9

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Voice & Music, Snapdragon Wearables		
			CVE ID : CVE-2021-1920		
Out-of- bounds Read	08-Sep-21	3.6	Buffer over read could occur due to incorrect check of buffer size while flashing emmc devices in Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking	https://www. qualcomm.co m/company/ product- security/bull etins/august- 2021-bulletin	0-QUA-QCA6- 200921/2717
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	08-Sep-21	10	CVE ID : CVE-2021-1928 Possible buffer overflow due to improper validation of device types during P2P search in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Woice & Music, Snapdragon Wired Infrastructure and Networking CVE ID : CVE-2021-1972	https://www. qualcomm.co m/company/ product- security/bull etins/august- 2021-bulletin	0-QUA-QCA6- 200921/2718
qca6335_firm	nware				
Exposure of Resource to Wrong Sphere	08-Sep-21	2.1	Child process can leak information from parent process due to numeric pids are getting compared and these pid can be reused in Snapdragon Auto,	https://www. qualcomm.co m/company/ product- security/bull etins/august-	0-QUA-QCA6- 200921/2719
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 & CVE ID	Patch	NCIIPC ID
			Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables	2021-bulletin	
			CVE ID : CVE-2021-1904		
Loop with Unreachable Exit Condition ('Infinite Loop')	08-Sep-21	5	Loop with unreachable exit condition may occur due to improper handling of unsupported input in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Voice & Music, Snapdragon Wearables CVE ID : CVE-2021-1914	https://www. qualcomm.co m/company/ product- security/bull etins/august- 2021-bulletin	0-QUA-QCA6- 200921/2720
Out-of- bounds Write	08-Sep-21	10	Possible buffer underflow due to lack of check for negative indices values when processing user provided input in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Voice & Music, Snapdragon Wearables CVE ID : CVE-2021-1916	https://www. qualcomm.co m/company/ product- security/bull etins/august- 2021-bulletin	0-QUA-QCA6- 200921/2721
Integer Underflow (Wrap or Wraparoun	08-Sep-21	10	Integer underflow can occur when the RTCP length is lesser than than the actual blocks present in Snapdragon	https://www. qualcomm.co m/company/ product-	0-QUA-QCA6- 200921/2722

CVSS Scoring Scale	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10
Page 1076 of 1474										

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
d)			Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Voice & Music, Snapdragon Wearables	security/bull etins/august- 2021-bulletin	
			CVE ID : CVE-2021-1919		
Integer Underflow (Wrap or Wraparoun d)	08-Sep-21	10	Integer underflow can occur due to improper handling of incoming RTCP packets in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Voice & Music, Snapdragon Wearables CVE ID : CVE-2021-1920	https://www. qualcomm.co m/company/ product- security/bull etins/august- 2021-bulletin	0-QUA-QCA6- 200921/2723
Out-of- bounds Read	08-Sep-21	3.6	Buffer over read could occur due to incorrect check of buffer size while flashing emmc devices in Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking CVE ID : CVE-2021-1928	https://www. qualcomm.co m/company/ product- security/bull etins/august- 2021-bulletin	0-QUA-QCA6- 200921/2724
Buffer Copy without Checking Size of Input ('Classic	08-Sep-21	10	Possible buffer overflow due to improper validation of device types during P2P search in Snapdragon Auto, Snapdragon Compute,	https://www. qualcomm.co m/company/ product- security/bull	0-QUA-QCA6- 200921/2725

0-1

1-2

2-3 3-4 4-5 Page 1077 of 1474 7-8

5-6

6-7

8-9

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID	
Buffer Overflow')			Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking CVE ID : CVE-2021-1972	etins/august- 2021-bulletin		
qca6390_firm	nware			1		
Exposure of Resource to Wrong Sphere	08-Sep-21	2.1	Child process can leak information from parent process due to numeric pids are getting compared and these pid can be reused in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wearables CVE ID : CVE-2021-1904	https://www. qualcomm.co m/company/ product- security/bull etins/august- 2021-bulletin	0-QUA-QCA6- 200921/2726	
Loop with Unreachable Exit Condition ('Infinite Loop')	08-Sep-21	5	Loop with unreachable exit condition may occur due to improper handling of unsupported input in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Voice & Music, Snapdragon Wearables CVE ID : CVE-2021-1914	https://www. qualcomm.co m/company/ product- security/bull etins/august- 2021-bulletin	0-QUA-QCA6- 200921/2727	
CVSS Scoring Scale 0-1 1-2 2-3 3-4 4-5 5-6 6-7 7-8 8-9 9-10						

 3-4
 4-5
 5-6
 6-7

 Page 1078 of 1474

Out-of- bounds Write08-Sep-21Image is a separation of the security o	Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Integer Underflow (Wrap or W)08-Sep-2110Integer underflow can occur when the RTCP length is lesser than than the actual blocks present in Snapdragon Auto, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Industrial IOT, Snapdragon Industrial IOT, Snapdragon Industrial IOT, Snapdragon Industrial IOT, Snapdragon Compute, Snapdragon Compute, Snapdragon Industrial IOT, Snapdragon Compute, Snapdragon Compute, Snapdragon Consumer IOT, Snapdragon Industrial IOT	bounds	08-Sep-21	10	due to lack of check for negative indices values when processing user provided input in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Voice & Music, Snapdragon Wearables	qualcomm.co m/company/ product- security/bull etins/august-	e e
Integer Underflow (Wrap or d)08-Sep-2110due to improper handling of incoming RTCP packets in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Industrial IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Voice & Music, Snapdragonhttps://www. qualcomm.co m/company/ product- security/bull etins/august- 2021-bulletin0-QUA-QCA6- 200921/2730	Underflow (Wrap or Wraparoun	08-Sep-21	10	Integer underflow can occur when the RTCP length is lesser than than the actual blocks present in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Voice & Music, Snapdragon Wearables	qualcomm.co m/company/ product- security/bull etins/august-	
Incorrect 08-Sep-21 46 Incorrect pointer argument https://www. 0.0014.0CA/	Underflow (Wrap or Wraparoun	08-Sep-21	10	due to improper handling of incoming RTCP packets in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Voice & Music, Snapdragon Wearables	qualcomm.co m/company/ product- security/bull etins/august-	
incorrect of sep 21 incorrect pointer argument intps://www. O-QUA-QCA6-	Incorrect	08-Sep-21	4.6	Incorrect pointer argument	https://www.	0-QUA-QCA6-

 3-4
 4-5
 5-6
 6-7

 Page 1079 of 1474

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Type Conversion or Cast			passed to trusted application TA could result in un- intended memory operations in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Industrial IOT CVE ID : CVE-2021-1923	qualcomm.co m/company/ product- security/bull etins/august- 2021-bulletin	200921/2731
Exposure of Resource to Wrong Sphere	08-Sep-21	2.1	Lack of strict validation of bootmode can lead to information disclosure in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wearables CVE ID : CVE-2021-1929	https://www. qualcomm.co m/company/ product- security/bull etins/august- 2021-bulletin	0-QUA-QCA6- 200921/2732
Improper Restriction of Operations within the Bounds of a Memory Buffer	08-Sep-21	3.6	Possible out of bounds read due to incorrect validation of incoming buffer length in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile CVE ID : CVE-2021-1930	https://www. qualcomm.co m/company/ product- security/bull etins/august- 2021-bulletin	0-QUA-QCA6- 200921/2733
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	08-Sep-21	10	Possible buffer overflow due to improper validation of device types during P2P search in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile,	https://www. qualcomm.co m/company/ product- security/bull etins/august- 2021-bulletin	0-QUA-QCA6- 200921/2734

0-1 1-2

5-6

6-7

7-8

8-9

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking		
			CVE ID : CVE-2021-1972		
qca6391_firm	nware			I	
Exposure of Resource to Wrong Sphere	08-Sep-21	2.1	Child process can leak information from parent process due to numeric pids are getting compared and these pid can be reused in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wearables CVE ID : CVE-2021-1904	https://www. qualcomm.co m/company/ product- security/bull etins/august- 2021-bulletin	0-QUA-QCA6- 200921/2735
Loop with Unreachable Exit Condition ('Infinite Loop')	08-Sep-21	5	Loop with unreachable exit condition may occur due to improper handling of unsupported input in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Voice & Music, Snapdragon Wearables CVE ID : CVE-2021-1914	https://www. qualcomm.co m/company/ product- security/bull etins/august- 2021-bulletin	0-QUA-QCA6- 200921/2736
Out-of- bounds Write	08-Sep-21	10	Possible buffer underflow due to lack of check for negative indices values when processing user provided	https://www. qualcomm.co m/company/ product-	0-QUA-QCA6- 200921/2737
CVSS Scoring Sc	ale 0-1	1-2	2-3 3-4 4-5 5-6	6-7 7-8	8-9 9-10

Page 1081 of 1474

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			input in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Voice & Music, Snapdragon Wearables CVE ID : CVE-2021-1916	security/bull etins/august- 2021-bulletin	
Integer Underflow (Wrap or Wraparoun d)	08-Sep-21	10	Integer underflow can occur when the RTCP length is lesser than than the actual blocks present in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Voice & Music, Snapdragon Wearables CVE ID : CVE-2021-1919	https://www. qualcomm.co m/company/ product- security/bull etins/august- 2021-bulletin	0-QUA-QCA6- 200921/2738
Integer Underflow (Wrap or Wraparoun d)	08-Sep-21	10	Integer underflow can occur due to improper handling of incoming RTCP packets in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Voice & Music, Snapdragon Wearables CVE ID : CVE-2021-1920	https://www. qualcomm.co m/company/ product- security/bull etins/august- 2021-bulletin	0-QUA-QCA6- 200921/2739
Incorrect Type Conversion or Cast	08-Sep-21	4.6	Incorrect pointer argument passed to trusted application TA could result in un- intended memory operations in Snapdragon Auto,	https://www. qualcomm.co m/company/ product- security/bull	0-QUA-QCA6- 200921/2740

CVSS Scoring Scale	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10
			Pa	age 1082 (of 1474					

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Snapdragon Compute, Snapdragon Connectivity, Snapdragon Industrial IOT CVE ID : CVE-2021-1923	etins/august- 2021-bulletin	
Exposure of Resource to Wrong Sphere	08-Sep-21	2.1	Lack of strict validation of bootmode can lead to information disclosure in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wearables	https://www. qualcomm.co m/company/ product- security/bull etins/august- 2021-bulletin	O-QUA-QCA6- 200921/2741
Improper Restriction of Operations within the Bounds of a Memory Buffer	08-Sep-21	3.6	CVE ID : CVE-2021-1929 Possible out of bounds read due to incorrect validation of incoming buffer length in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile CVE ID : CVE-2021-1930	https://www. qualcomm.co m/company/ product- security/bull etins/august- 2021-bulletin	0-QUA-QCA6- 200921/2742
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	08-Sep-21	10	Possible buffer overflow due to improper validation of device types during P2P search in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Woice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and	https://www. qualcomm.co m/company/ product- security/bull etins/august- 2021-bulletin	O-QUA-QCA6- 200921/2743

0-1

1-2

5-6

6-7

7-8

8-9

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Networking		
			CVE ID : CVE-2021-1972		
qca6420_firn	nware				
Exposure of Resource to Wrong Sphere	08-Sep-21	2.1	Child process can leak information from parent process due to numeric pids are getting compared and these pid can be reused in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wearables CVE ID : CVE-2021-1904	https://www. qualcomm.co m/company/ product- security/bull etins/august- 2021-bulletin	0-QUA-QCA6- 200921/2744
Loop with Unreachable Exit Condition ('Infinite Loop')	08-Sep-21	5	Loop with unreachable exit condition may occur due to improper handling of unsupported input in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Voice & Music, Snapdragon Wearables CVE ID : CVE-2021-1914	https://www. qualcomm.co m/company/ product- security/bull etins/august- 2021-bulletin	0-QUA-QCA6- 200921/2745
Out-of- bounds Write	08-Sep-21	10	Possible buffer underflow due to lack of check for negative indices values when processing user provided input in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT,	https://www. qualcomm.co m/company/ product- security/bull etins/august- 2021-bulletin	0-QUA-QCA6- 200921/2746
CVSS Scoring Sc	ale 0-1	1-2	2-3 3-4 4-5 5-6	6-7 7-8	8-9 9-10

Page 1084 of 1474

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Voice & Music, Snapdragon Wearables		
			CVE ID : CVE-2021-1916		
Integer Underflow (Wrap or Wraparoun d)	08-Sep-21	10	Integer underflow can occur when the RTCP length is lesser than than the actual blocks present in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Voice & Music, Snapdragon Wearables CVE ID : CVE-2021-1919	https://www. qualcomm.co m/company/ product- security/bull etins/august- 2021-bulletin	0-QUA-QCA6- 200921/2747
Integer Underflow (Wrap or Wraparoun d)	08-Sep-21	10	Integer underflow can occur due to improper handling of incoming RTCP packets in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Voice & Music, Snapdragon Wearables CVE ID : CVE-2021-1920	https://www. qualcomm.co m/company/ product- security/bull etins/august- 2021-bulletin	0-QUA-QCA6- 200921/2748
			Incorrect pointer argument		
Incorrect Type Conversion or Cast	08-Sep-21	4.6	passed to trusted application TA could result in un- intended memory operations in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Industrial IOT CVE ID : CVE-2021-1923	https://www. qualcomm.co m/company/ product- security/bull etins/august- 2021-bulletin	0-QUA-QCA6- 200921/2749
CVSS Scoring Sc	ale 0-1	1-2	2-3 3-4 4-5 5-6 Page 1085 of 1474	6-7 7-8	8-9 9-10

Page 1085 of 1474

	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Exposure of Resource to Wrong Sphere	08-Sep-21	2.1	Lack of strict validation of bootmode can lead to information disclosure in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wearables CVE ID : CVE-2021-1929	https://www. qualcomm.co m/company/ product- security/bull etins/august- 2021-bulletin	0-QUA-QCA6- 200921/2750
Improper Restriction of Operations within the Bounds of a Memory Buffer	08-Sep-21	3.6	Possible out of bounds read due to incorrect validation of incoming buffer length in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile CVE ID : CVE-2021-1930	https://www. qualcomm.co m/company/ product- security/bull etins/august- 2021-bulletin	0-QUA-QCA6- 200921/2751
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	08-Sep-21	10	Possible buffer overflow due to improper validation of device types during P2P search in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Industrial IOT, Snapdragon Woice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking CVE ID : CVE-2021-1972	https://www. qualcomm.co m/company/ product- security/bull etins/august- 2021-bulletin	0-QUA-QCA6- 200921/2752
	nware				
qca6421_firm	in the c				

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Resource to Wrong Sphere			information from parent process due to numeric pids are getting compared and these pid can be reused in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wearables CVE ID : CVE-2021-1904	qualcomm.co m/company/ product- security/bull etins/august- 2021-bulletin	200921/2753
Loop with Unreachable Exit Condition ('Infinite Loop')	08-Sep-21	5	Loop with unreachable exit condition may occur due to improper handling of unsupported input in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Voice & Music, Snapdragon Wearables CVE ID : CVE-2021-1914	https://www. qualcomm.co m/company/ product- security/bull etins/august- 2021-bulletin	0-QUA-QCA6- 200921/2754
Out-of- bounds Write	08-Sep-21	10	Possible buffer underflow due to lack of check for negative indices values when processing user provided input in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Voice & Music, Snapdragon Wearables	https://www. qualcomm.co m/company/ product- security/bull etins/august- 2021-bulletin	0-QUA-QCA6- 200921/2755

CVSS Scoring Scale	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10
			Pa	age 1087	of 1474					

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2021-1916		
Integer Underflow (Wrap or Wraparoun d)	08-Sep-21	10	Integer underflow can occur when the RTCP length is lesser than than the actual blocks present in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Voice & Music, Snapdragon Wearables CVE ID : CVE-2021-1919	https://www. qualcomm.co m/company/ product- security/bull etins/august- 2021-bulletin	0-QUA-QCA6- 200921/2756
Integer Underflow (Wrap or Wraparoun d)	08-Sep-21	10	Integer underflow can occur due to improper handling of incoming RTCP packets in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Voice & Music, Snapdragon Wearables CVE ID : CVE-2021-1920	https://www. qualcomm.co m/company/ product- security/bull etins/august- 2021-bulletin	0-QUA-QCA6- 200921/2757
Incorrect Type Conversion or Cast	08-Sep-21	4.6	Incorrect pointer argument passed to trusted application TA could result in un- intended memory operations in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Industrial IOT CVE ID : CVE-2021-1923	https://www. qualcomm.co m/company/ product- security/bull etins/august- 2021-bulletin	0-QUA-QCA6- 200921/2758
Exposure of Resource to Wrong Sphere CVSS Scoring Sc	08-Sep-21 ale 0-1	2.1	Lack of strict validation of bootmode can lead to information disclosure in Snapdragon Auto, 2-3 3-4 4-5 5-6	https://www. qualcomm.co m/company/ product-	0-QUA-QCA6- 200921/2759 8-9 9-10

Page 1088 of 1474

		Snapdragon Compute,	cocurity/hull	
		Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wearables	security/bull etins/august- 2021-bulletin	
08-Sep-21	3.6	Possible out of bounds read due to incorrect validation of incoming buffer length in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile CVE ID : CVE-2021-1930	https://www. qualcomm.co m/company/ product- security/bull etins/august- 2021-bulletin	0-QUA-QCA6- 200921/2760
08-Sep-21	10	Possible buffer overflow due to improper validation of device types during P2P search in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Woice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking CVE ID : CVE-2021-1972	https://www. qualcomm.co m/company/ product- security/bull etins/august- 2021-bulletin	0-QUA-QCA6- 200921/2761
ware				
08-Sep-21	2.1	Child process can leak information from parent process due to numeric pids are getting compared and these pid can be reused in	https://www. qualcomm.co m/company/ product- security/bull	0-QUA-QCA6- 200921/2762
	08-Sep-21	08-Sep-21 10 ware	Napdragon Mobile, Snapdragon WearablesCVE ID : CVE-2021-192908-Sep-213.68.6Possible out of bounds read due to incorrect validation of incoming buffer length in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile08-Sep-213.69.8-Sep-21Possible buffer overflow due to improper validation of device types during P2P search in Snapdragon Auto, Snapdragon Consumer IOT, Snapdragon Consumer IOT, Snapdragon Compute, Snapdragon Compute, Snapdragon Consumer IOT, Snapdragon Mobile, Snapdragon Mobile, Snapdragon Wired Infrastructure and Networking08-Sep-21Child process can leak information from parent process due to numeric pids are getting compared and	Napdragon Mobile, Snapdragon WearablesSnapdragon WearablesCVE ID : CVE-2021-1929CVE ID : CVE-2021-192908-Sep-213.6Possible out of bounds read due to incorrect validation of incoming buffer length in Snapdragon Auto, Snapdragon Compute, Snapdragon Consectivity, Snapdragon Industrial IOT, Snapdragon Mobilehttps://www. qualcomm.co m/company/ product- security/bull etins/august- 2021-bulletin08-Sep-2110Possible buffer overflow due to improper validation of device types during P2P search in Snapdragon Consumer IOT, Snapdragon Consumer IOT, Snapdragon Consumer IOT, Snapdragon Consumer IOT, Snapdragon Consumer IOT, Snapdragon Mobile, Snapdragon Consumer IOT, Snapdragon Voice & Music, Snapdragon Voice & Music, Snapdragon Wired Infrastructure and Networkinghttps://www. qualcomm.co m/company/ product- security/bull etins/august- 2021-bulletin08-Sep-212.1Child process can leak information from parent process due to numeric pids are getting compared andhttps://www. qualcomm.co m/company/ product-

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables CVE ID : CVE-2021-1904	etins/august- 2021-bulletin	
Loop with Unreachable Exit Condition ('Infinite Loop')	08-Sep-21	5	Loop with unreachable exit condition may occur due to improper handling of unsupported input in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Voice & Music, Snapdragon Wearables CVE ID : CVE-2021-1914	https://www. qualcomm.co m/company/ product- security/bull etins/august- 2021-bulletin	0-QUA-QCA6- 200921/2763
Out-of- bounds Write	08-Sep-21	10	Possible buffer underflow due to lack of check for negative indices values when processing user provided input in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Voice & Music, Snapdragon Wearables CVE ID : CVE-2021-1916	https://www. qualcomm.co m/company/ product- security/bull etins/august- 2021-bulletin	0-QUA-QCA6- 200921/2764
Integer Underflow (Wrap or	08-Sep-21	10	Integer underflow can occur when the RTCP length is lesser than than the actual	https://www. qualcomm.co m/company/	0-QUA-QCA6- 200921/2765

CVSS Scoring Scale	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10
			Ра	ge 1090 (of 1474					

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Wraparoun d)			blocks present in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Voice & Music, Snapdragon Wearables CVE ID : CVE-2021-1919	product- security/bull etins/august- 2021-bulletin	
Integer Underflow (Wrap or Wraparoun d)	08-Sep-21	10	Integer underflow can occur due to improper handling of incoming RTCP packets in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Voice & Music, Snapdragon Wearables CVE ID : CVE-2021-1920	https://www. qualcomm.co m/company/ product- security/bull etins/august- 2021-bulletin	0-QUA-QCA6- 200921/2766
Incorrect Type Conversion or Cast	08-Sep-21	4.6	Incorrect pointer argument passed to trusted application TA could result in un- intended memory operations in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Industrial IOT CVE ID : CVE-2021-1923	https://www. qualcomm.co m/company/ product- security/bull etins/august- 2021-bulletin	0-QUA-QCA6- 200921/2767
Exposure of Resource to Wrong Sphere	08-Sep-21	2.1	Lack of strict validation of bootmode can lead to information disclosure in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT,	https://www. qualcomm.co m/company/ product- security/bull etins/august- 2021-bulletin	0-QUA-QCA6- 200921/2768

0-1

5-6

6-7

7-8

8-9

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Snapdragon Mobile, Snapdragon Wearables CVE ID : CVE-2021-1929		
Improper Restriction of Operations within the Bounds of a Memory Buffer	08-Sep-21	3.6	Possible out of bounds read due to incorrect validation of incoming buffer length in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile CVE ID : CVE-2021-1930	https://www. qualcomm.co m/company/ product- security/bull etins/august- 2021-bulletin	0-QUA-QCA6- 200921/2769
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	08-Sep-21	10	Possible buffer overflow due to improper validation of device types during P2P search in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Woice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking CVE ID : CVE-2021-1972	https://www. qualcomm.co m/company/ product- security/bull etins/august- 2021-bulletin	0-QUA-QCA6- 200921/2770
qca6428_firm	nware				
Out-of- bounds Read	08-Sep-21	3.6	Buffer over read could occur due to incorrect check of buffer size while flashing emmc devices in Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon	https://www. qualcomm.co m/company/ product- security/bull etins/august- 2021-bulletin	0-QUA-QCA6- 200921/2771

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Wearables, Snapdragon Wired Infrastructure and Networking		
			CVE ID : CVE-2021-1928		
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	08-Sep-21	10	Possible buffer overflow due to improper validation of device types during P2P search in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Woice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking CVE ID : CVE-2021-1972	https://www. qualcomm.co m/company/ product- security/bull etins/august- 2021-bulletin	0-QUA-QCA6- 200921/2772
qca6430_firm	nware				
Exposure of Resource to Wrong Sphere	08-Sep-21	2.1	Child process can leak information from parent process due to numeric pids are getting compared and these pid can be reused in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables CVE ID : CVE-2021-1904	https://www. qualcomm.co m/company/ product- security/bull etins/august- 2021-bulletin	0-QUA-QCA6- 200921/2773
Loop with Unreachable Exit Condition	08-Sep-21	5	Loop with unreachable exit condition may occur due to improper handling of unsupported input in	https://www. qualcomm.co m/company/ product-	0-QUA-QCA6- 200921/2774
CVSS Scoring Sc	ale 0-1	1-2	2-3 3-4 4-5 5-6	6-7 7-8	8-9 9-10

Page 1093 of 1474

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
('Infinite Loop')			Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Voice & Music, Snapdragon Wearables	security/bull etins/august- 2021-bulletin	
Out-of- bounds Write	08-Sep-21	10	CVE ID : CVE-2021-1914 Possible buffer underflow due to lack of check for negative indices values when processing user provided input in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Voice & Music, Snapdragon Wearables CVE ID : CVE-2021-1916	https://www. qualcomm.co m/company/ product- security/bull etins/august- 2021-bulletin	0-QUA-QCA6- 200921/2775
Integer Underflow (Wrap or Wraparoun d)	08-Sep-21	10	Integer underflow can occur when the RTCP length is lesser than than the actual blocks present in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Voice & Music, Snapdragon Wearables CVE ID : CVE-2021-1919	https://www. qualcomm.co m/company/ product- security/bull etins/august- 2021-bulletin	0-QUA-QCA6- 200921/2776
Integer Underflow (Wrap or Wraparoun	08-Sep-21	10	Integer underflow can occur due to improper handling of incoming RTCP packets in Snapdragon Auto,	https://www. qualcomm.co m/company/ product-	0-QUA-QCA6- 200921/2777

CVSS Scoring Scale	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10
			De	a 1004	of 1 1 7 1					

d)			Snapdragon Compute,	security/bull	
			Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Voice & Music, Snapdragon Wearables CVE ID : CVE-2021-1920	etins/august- 2021-bulletin	
Incorrect Type Conversion or Cast	08-Sep-21	4.6	Incorrect pointer argument passed to trusted application TA could result in un- intended memory operations in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Industrial IOT CVE ID : CVE-2021-1923	https://www. qualcomm.co m/company/ product- security/bull etins/august- 2021-bulletin	0-QUA-QCA6- 200921/2778
Exposure of Resource to Wrong Sphere	08-Sep-21	2.1	Lack of strict validation of bootmode can lead to information disclosure in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wearables CVE ID : CVE-2021-1929	https://www. qualcomm.co m/company/ product- security/bull etins/august- 2021-bulletin	0-QUA-QCA6- 200921/2779
Improper Restriction of Operations within the Bounds of a Memory Buffer	08-Sep-21	3.6	Possible out of bounds read due to incorrect validation of incoming buffer length in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile CVE ID : CVE-2021-1930	https://www. qualcomm.co m/company/ product- security/bull etins/august- 2021-bulletin	0-QUA-QCA6- 200921/2780

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	08-Sep-21	10	Possible buffer overflow due to improper validation of device types during P2P search in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Woice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking CVE ID : CVE-2021-1972	https://www. qualcomm.co m/company/ product- security/bull etins/august- 2021-bulletin	0-QUA-QCA6- 200921/2781
qca6431_firm	nware				
Exposure of Resource to Wrong Sphere	08-Sep-21	2.1	Child process can leak information from parent process due to numeric pids are getting compared and these pid can be reused in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables CVE ID : CVE-2021-1904	https://www. qualcomm.co m/company/ product- security/bull etins/august- 2021-bulletin	0-QUA-QCA6- 200921/2782
Loop with Unreachable Exit Condition ('Infinite Loop')	08-Sep-21	5	Loop with unreachable exit condition may occur due to improper handling of unsupported input in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT,	https://www. qualcomm.co m/company/ product- security/bull etins/august- 2021-bulletin	0-QUA-QCA6- 200921/2783

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Snapdragon IoT, Snapdragon Voice & Music, Snapdragon Wearables		
			CVE ID : CVE-2021-1914		
Out-of- bounds Write	08-Sep-21	10	Possible buffer underflow due to lack of check for negative indices values when processing user provided input in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Voice & Music, Snapdragon Wearables	https://www. qualcomm.co m/company/ product- security/bull etins/august- 2021-bulletin	0-QUA-QCA6- 200921/2784
			CVE ID : CVE-2021-1916		
Integer Underflow (Wrap or Wraparoun d)	08-Sep-21	10	Integer underflow can occur when the RTCP length is lesser than than the actual blocks present in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Voice & Music, Snapdragon Wearables	https://www. qualcomm.co m/company/ product- security/bull etins/august- 2021-bulletin	O-QUA-QCA6- 200921/2785
			CVE ID : CVE-2021-1919		
Integer Underflow (Wrap or Wraparoun d)	08-Sep-21	10	Integer underflow can occur due to improper handling of incoming RTCP packets in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon	https://www. qualcomm.co m/company/ product- security/bull etins/august- 2021-bulletin	O-QUA-QCA6- 200921/2786

0-1

1-2

3-4 2-3 Page 1097 of 1474

4-5

5-6

6-7

7-8

8-9

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Voice & Music, Snapdragon Wearables		
			CVE ID : CVE-2021-1920		
Incorrect Type Conversion or Cast	08-Sep-21	4.6	Incorrect pointer argument passed to trusted application TA could result in un- intended memory operations in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Industrial IOT CVE ID : CVE-2021-1923	https://www. qualcomm.co m/company/ product- security/bull etins/august- 2021-bulletin	0-QUA-QCA6- 200921/2787
Exposure of Resource to Wrong Sphere	08-Sep-21	2.1	Lack of strict validation of bootmode can lead to information disclosure in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wearables CVE ID : CVE-2021-1929	https://www. qualcomm.co m/company/ product- security/bull etins/august- 2021-bulletin	0-QUA-QCA6- 200921/2788
Improper Restriction of Operations within the Bounds of a Memory Buffer	08-Sep-21	3.6	Possible out of bounds read due to incorrect validation of incoming buffer length in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile CVE ID : CVE-2021-1930	https://www. qualcomm.co m/company/ product- security/bull etins/august- 2021-bulletin	0-QUA-QCA6- 200921/2789
Buffer Copy without Checking Size of Input ('Classic CVSS Scoring Sc	08-Sep-21	10	Possible buffer overflow dueto improper validation ofdevice types during P2Psearch in Snapdragon Auto,Snapdragon Compute,2-33-44-55-6	https://www. qualcomm.co m/company/ product- security/bull 6-7 7-8	0-QUA-QCA6- 200921/2790 8-9 9-10

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Buffer Overflow')			Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking CVE ID : CVE-2021-1972	etins/august- 2021-bulletin	
qca6436_firr	nware				
Exposure of Resource to Wrong Sphere	08-Sep-21	2.1	Child process can leak information from parent process due to numeric pids are getting compared and these pid can be reused in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wearables CVE ID : CVE-2021-1904	https://www. qualcomm.co m/company/ product- security/bull etins/august- 2021-bulletin	0-QUA-QCA6- 200921/2791
Loop with Unreachable Exit Condition ('Infinite Loop')	08-Sep-21	5	Loop with unreachable exit condition may occur due to improper handling of unsupported input in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Voice & Music, Snapdragon Wearables CVE ID : CVE-2021-1914	https://www. qualcomm.co m/company/ product- security/bull etins/august- 2021-bulletin	0-QUA-QCA6- 200921/2792

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Out-of- bounds Write	08-Sep-21	10	Possible buffer underflow due to lack of check for negative indices values when processing user provided input in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Voice & Music, Snapdragon Wearables	https://www. qualcomm.co m/company/ product- security/bull etins/august- 2021-bulletin	0-QUA-QCA6- 200921/2793
Integer Underflow (Wrap or Wraparoun d)	08-Sep-21	10	CVE ID : CVE-2021-1916 Integer underflow can occur when the RTCP length is lesser than than the actual blocks present in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Voice & Music, Snapdragon Wearables CVE ID : CVE-2021-1919	https://www. qualcomm.co m/company/ product- security/bull etins/august- 2021-bulletin	0-QUA-QCA6- 200921/2794
Integer Underflow (Wrap or Wraparoun d)	08-Sep-21	10	Integer underflow can occur due to improper handling of incoming RTCP packets in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Voice & Music, Snapdragon Wearables CVE ID : CVE-2021-1920	https://www. qualcomm.co m/company/ product- security/bull etins/august- 2021-bulletin	0-QUA-QCA6- 200921/2795
Incorrect	08-Sep-21	4.6	Incorrect pointer argument	https://www.	0-QUA-QCA6-

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Type Conversion or Cast			passed to trusted application TA could result in un- intended memory operations in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Industrial IOT CVE ID : CVE-2021-1923	qualcomm.co m/company/ product- security/bull etins/august- 2021-bulletin	200921/2796
Exposure of Resource to Wrong Sphere	08-Sep-21	2.1	Lack of strict validation of bootmode can lead to information disclosure in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wearables CVE ID : CVE-2021-1929	https://www. qualcomm.co m/company/ product- security/bull etins/august- 2021-bulletin	0-QUA-QCA6- 200921/2797
Improper Restriction of Operations within the Bounds of a Memory Buffer	08-Sep-21	3.6	Possible out of bounds read due to incorrect validation of incoming buffer length in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile CVE ID : CVE-2021-1930	https://www. qualcomm.co m/company/ product- security/bull etins/august- 2021-bulletin	0-QUA-QCA6- 200921/2798
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	08-Sep-21	10	Possible buffer overflow due to improper validation of device types during P2P search in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile,	https://www. qualcomm.co m/company/ product- security/bull etins/august- 2021-bulletin	0-QUA-QCA6- 200921/2799

0-1

1-2 2-3

5-6

6-7

7-8

8-9

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking		
qca6438_firm	nwaro		CVE ID : CVE-2021-1972		
Out-of- bounds Read	08-Sep-21	3.6	Buffer over read could occur due to incorrect check of buffer size while flashing emmc devices in Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking	https://www. qualcomm.co m/company/ product- security/bull etins/august- 2021-bulletin	O-QUA-QCA6- 200921/2800
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	08-Sep-21	10	CVE ID : CVE-2021-1928 Possible buffer overflow due to improper validation of device types during P2P search in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Woice & Music, Snapdragon Wired Infrastructure and Networking CVE ID : CVE-2021-1972	https://www. qualcomm.co m/company/ product- security/bull etins/august- 2021-bulletin	O-QUA-QCA6- 200921/2801
qca6564au_f	irmware				
Exposure of Resource to	08-Sep-21	2.1	Child process can leak information from parent	https://www. qualcomm.co	0-QUA-QCA6-
CVSS Scoring Sc	ale 0-1	1-2	2-3 3-4 4-5 5-6 Page 1102 of 1474	6-7 7-8	8-9 9-10

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Wrong Sphere			process due to numeric pids are getting compared and these pid can be reused in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wearables CVE ID : CVE-2021-1904	m/company/ product- security/bull etins/august- 2021-bulletin	200921/2802
Loop with Unreachable Exit Condition ('Infinite Loop')	08-Sep-21	5	Loop with unreachable exit condition may occur due to improper handling of unsupported input in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Voice & Music, Snapdragon Wearables CVE ID : CVE-2021-1914	https://www. qualcomm.co m/company/ product- security/bull etins/august- 2021-bulletin	0-QUA-QCA6- 200921/2803
Out-of- bounds Write	08-Sep-21	10	Possible buffer underflow due to lack of check for negative indices values when processing user provided input in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Voice & Music, Snapdragon Wearables CVE ID : CVE-2021-1916	https://www. qualcomm.co m/company/ product- security/bull etins/august- 2021-bulletin	O-QUA-QCA6- 200921/2804

[CVSS Scoring Scale	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10
	Page 1102 of 1474										

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Integer Underflow (Wrap or Wraparoun d)	08-Sep-21	10	Integer underflow can occur when the RTCP length is lesser than than the actual blocks present in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Voice & Music, Snapdragon Wearables	https://www. qualcomm.co m/company/ product- security/bull etins/august- 2021-bulletin	O-QUA-QCA6- 200921/2805
			CVE ID : CVE-2021-1919		
Integer Underflow (Wrap or Wraparoun d)	08-Sep-21	10	Integer underflow can occur due to improper handling of incoming RTCP packets in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Voice & Music, Snapdragon Wearables	https://www. qualcomm.co m/company/ product- security/bull etins/august- 2021-bulletin	0-QUA-QCA6- 200921/2806
			CVE ID : CVE-2021-1920		
Exposure of Resource to Wrong Sphere	08-Sep-21	2.1	Lack of strict validation of bootmode can lead to information disclosure in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wearables	https://www. qualcomm.co m/company/ product- security/bull etins/august- 2021-bulletin	O-QUA-QCA6- 200921/2807
			CVE ID : CVE-2021-1929		
Improper Restriction of	08-Sep-21	3.6	Possible out of bounds read due to incorrect validation of incoming buffer length in	https://www. qualcomm.co m/company/	0-QUA-QCA6- 200921/2808

CVSS Scoring Scale	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10
Dago 1104 of 1474										

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Operations within the Bounds of a Memory Buffer			Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile	product- security/bull etins/august- 2021-bulletin	
			CVE ID : CVE-2021-1930		
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	08-Sep-21	10	Possible buffer overflow due to improper validation of device types during P2P search in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Industrial IOT, Snapdragon Woice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking CVE ID : CVE-2021-1972	https://www. qualcomm.co m/company/ product- security/bull etins/august- 2021-bulletin	0-QUA-QCA6- 200921/2809
qca6564a_fir	mware				
Exposure of Resource to Wrong Sphere	08-Sep-21	2.1	Child process can leak information from parent process due to numeric pids are getting compared and these pid can be reused in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wearables CVE ID : CVE-2021-1904	https://www. qualcomm.co m/company/ product- security/bull etins/august- 2021-bulletin	0-QUA-QCA6- 200921/2810
				1	

		condition may occur due to	qualcomm.co	200921/2811
		improper handling of unsupported input in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Voice & Music, Snapdragon Wearables	m/company/ product- security/bull etins/august- 2021-bulletin	
8-Sep-21	10	due to lack of check for negative indices values when processing user provided input in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Voice & Music, Snapdragon Wearables	https://www. qualcomm.co m/company/ product- security/bull etins/august- 2021-bulletin	0-QUA-QCA6- 200921/2812
8-Sep-21	10	CVE ID : CVE-2021-1916 Integer underflow can occur when the RTCP length is lesser than than the actual blocks present in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Voice & Music, Snapdragon Wearables CVE ID : CVE-2021-1919	https://www. qualcomm.co m/company/ product- security/bull etins/august- 2021-bulletin	0-QUA-QCA6- 200921/2813
8-Sep-21	10	Integer underflow can occur	https://www.	0-QUA-QCA6-
E	3-Sep-21	3-Sep-21 10	B-Sep-2110Snapdragon Compute, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Voice & Music, Snapdragon WearablesB-Sep-2110Possible buffer underflow due to lack of check for negative indices values when processing user provided input in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer IOT, Snapdragon Consumer IOT, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Industrial IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Voice & Music, Snapdragon WearablesB-Sep-2110Image: underflow can occur when the RTCP length is lesser than than the actual blocks present in Snapdragon Auto, Snapdragon Consumer IOT, Snapdragon Consumer IOT, Snapdragon Consumer IOT, Snapdragon Consumer IOT, Snapdragon Consumer IOT, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Industrial IOT, Snapdragon Consumer IOT, Snapdragon Industrial IOT, <td>Snapdragon Compute, Snapdragon Connectivity, Snapdragon Industrial IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Voice & Music, Snapdragon Possible buffer underflow due to lack of check for negative indices values when processing user provided input in Snapdragon Auto, Snapdragon Conpute, Snapdragon Iodustrial IOT, Snapdragon Industrial IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Voice & Music, Snapdragon CVE ID : CVE-2021-1916etins/august- 2021-bulletin tins/august- 2021-bulletin3-Sep-2110Integer underflow can occur when the RTCP length is lesser than than the actual blocks present in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Iot, Snapdragon Voice & Music, Snapdragon<br< td=""></br<></br></td>	Snapdragon Compute, Snapdragon Connectivity,

 3-4
 4-5
 5-6
 6-7

 Page 1106 of 1474

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID					
Underflow (Wrap or Wraparoun d)			due to improper handling of incoming RTCP packets in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Voice & Music, Snapdragon Wearables CVE ID : CVE-2021-1920	qualcomm.co m/company/ product- security/bull etins/august- 2021-bulletin	200921/2814					
Exposure of Resource to Wrong Sphere	08-Sep-21	2.1	Lack of strict validation of bootmode can lead to information disclosure in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wearables CVE ID : CVE-2021-1929	https://www. qualcomm.co m/company/ product- security/bull etins/august- 2021-bulletin	0-QUA-QCA6- 200921/2815					
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	08-Sep-21	10	Possible buffer overflow due to improper validation of device types during P2P search in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Woice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking CVE ID : CVE-2021-1972	https://www. qualcomm.co m/company/ product- security/bull etins/august- 2021-bulletin	O-QUA-QCA6- 200921/2816					
qca6564_firm	nware		CVE ID : CVE-2021-1972							
-										
CVSS Scoring Sc	ale 0-1	1-2	2-3 3-4 4-5 5-6 Page 1107 of 1474							

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Exposure of Resource to Wrong Sphere	08-Sep-21	2.1	Child process can leak information from parent process due to numeric pids are getting compared and these pid can be reused in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wearables CVE ID : CVE-2021-1904	https://www. qualcomm.co m/company/ product- security/bull etins/august- 2021-bulletin	0-QUA-QCA6- 200921/2817
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	08-Sep-21	10	Possible buffer overflow due to improper validation of device types during P2P search in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Industrial IOT, Snapdragon Woile, Snapdragon Woice & Music, Snapdragon Wired Infrastructure and Networking CVE ID : CVE-2021-1972	https://www. qualcomm.co m/company/ product- security/bull etins/august- 2021-bulletin	0-QUA-QCA6- 200921/2818
qca6574au_f	irmware				
Exposure of Resource to Wrong Sphere	08-Sep-21	2.1	Child process can leak information from parent process due to numeric pids are getting compared and these pid can be reused in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT,	https://www. qualcomm.co m/company/ product- security/bull etins/august- 2021-bulletin	0-QUA-QCA6- 200921/2819
CVSS Scoring Sc	ale 0-1	1-2	2-3 3-4 4-5 5-6 Page 1108 of 1474	6-7 7-8	8-9 9-10

Page 1108 of 1474

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables		
			CVE ID : CVE-2021-1904		
Loop with Unreachable Exit Condition ('Infinite Loop')	08-Sep-21	5	Loop with unreachable exit condition may occur due to improper handling of unsupported input in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Voice & Music, Snapdragon Wearables	https://www. qualcomm.co m/company/ product- security/bull etins/august- 2021-bulletin	O-QUA-QCA6- 200921/2820
			CVE ID : CVE-2021-1914		
Out-of- bounds Write	08-Sep-21	10	Possible buffer underflow due to lack of check for negative indices values when processing user provided input in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Voice & Music, Snapdragon Wearables CVE ID : CVE-2021-1916	https://www. qualcomm.co m/company/ product- security/bull etins/august- 2021-bulletin	0-QUA-QCA6- 200921/2821
Integer Underflow (Wrap or Wraparoun d)	08-Sep-21	10	Integer underflow can occur when the RTCP length is lesser than than the actual blocks present in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT,	https://www. qualcomm.co m/company/ product- security/bull etins/august- 2021-bulletin	O-QUA-QCA6- 200921/2822
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 & CVE ID	Patch	NCIIPC ID
			Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Voice & Music, Snapdragon Wearables CVE ID : CVE-2021-1919		
Integer Underflow (Wrap or Wraparoun d)	08-Sep-21	10	Integer underflow can occur due to improper handling of incoming RTCP packets in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Voice & Music, Snapdragon Wearables CVE ID : CVE-2021-1920	https://www. qualcomm.co m/company/ product- security/bull etins/august- 2021-bulletin	0-QUA-QCA6- 200921/2823
Incorrect Type Conversion or Cast	08-Sep-21	4.6	Incorrect pointer argument passed to trusted application TA could result in un- intended memory operations in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Industrial IOT CVE ID : CVE-2021-1923	https://www. qualcomm.co m/company/ product- security/bull etins/august- 2021-bulletin	0-QUA-QCA6- 200921/2824
Exposure of Resource to Wrong Sphere	08-Sep-21	2.1	Lack of strict validation of bootmode can lead to information disclosure in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wearables CVE ID : CVE-2021-1929	https://www. qualcomm.co m/company/ product- security/bull etins/august- 2021-bulletin	0-QUA-QCA6- 200921/2825

CVSS Scoring Scale	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10
Page 1110 of 1474										

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Improper Restriction of Operations within the Bounds of a Memory Buffer	08-Sep-21	3.6	Possible out of bounds read due to incorrect validation of incoming buffer length in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile CVE ID : CVE-2021-1930	https://www. qualcomm.co m/company/ product- security/bull etins/august- 2021-bulletin	0-QUA-QCA6- 200921/2826
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	08-Sep-21	10	Possible buffer overflow due to improper validation of device types during P2P search in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Woice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking CVE ID : CVE-2021-1972	https://www. qualcomm.co m/company/ product- security/bull etins/august- 2021-bulletin	0-QUA-QCA6- 200921/2827
qca6574a_fir	mware				
Exposure of Resource to Wrong Sphere	08-Sep-21	2.1	Child process can leak information from parent process due to numeric pids are getting compared and these pid can be reused in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music,	https://www. qualcomm.co m/company/ product- security/bull etins/august- 2021-bulletin	0-QUA-QCA6- 200921/2828

CVSS Scoring Scale	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10
Page 1111 of 1474										

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Snapdragon Wearables		
			CVE ID : CVE-2021-1904		
Loop with Unreachable Exit Condition ('Infinite Loop')	08-Sep-21	5	Loop with unreachable exit condition may occur due to improper handling of unsupported input in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Voice & Music, Snapdragon Wearables	https://www. qualcomm.co m/company/ product- security/bull etins/august- 2021-bulletin	0-QUA-QCA6- 200921/2829
			CVE ID : CVE-2021-1914		
Out-of- bounds Write	08-Sep-21	10	Possible buffer underflow due to lack of check for negative indices values when processing user provided input in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Voice & Music, Snapdragon Wearables	https://www. qualcomm.co m/company/ product- security/bull etins/august- 2021-bulletin	0-QUA-QCA6- 200921/2830
			CVE ID : CVE-2021-1916		
Integer Underflow (Wrap or Wraparoun d)	08-Sep-21	10	Integer underflow can occur when the RTCP length is lesser than than the actual blocks present in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Voice & Music, Snapdragon	https://www. qualcomm.co m/company/ product- security/bull etins/august- 2021-bulletin	0-QUA-QCA6- 200921/2831

0-1

1-2

3-4 2-3 Page 1112 of 1474

4-5

5-6

6-7

7-8

8-9

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Wearables		
			CVE ID : CVE-2021-1919		
Integer Underflow (Wrap or Wraparoun d)	08-Sep-21	10	Integer underflow can occur due to improper handling of incoming RTCP packets in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Voice & Music, Snapdragon Wearables	https://www. qualcomm.co m/company/ product- security/bull etins/august- 2021-bulletin	0-QUA-QCA6- 200921/2832
			CVE ID : CVE-2021-1920		
Incorrect Type Conversion or Cast	08-Sep-21	4.6	Incorrect pointer argument passed to trusted application TA could result in un- intended memory operations in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Industrial IOT CVE ID : CVE-2021-1923	https://www. qualcomm.co m/company/ product- security/bull etins/august- 2021-bulletin	0-QUA-QCA6- 200921/2833
Exposure of Resource to Wrong Sphere	08-Sep-21	2.1	Lack of strict validation of bootmode can lead to information disclosure in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wearables CVE ID : CVE-2021-1929	https://www. qualcomm.co m/company/ product- security/bull etins/august- 2021-bulletin	0-QUA-QCA6- 200921/2834
Improper Restriction of Operations	08-Sep-21	3.6	Possible out of bounds read due to incorrect validation of incoming buffer length in Snapdragon Auto,	https://www. qualcomm.co m/company/ product-	0-QUA-QCA6- 200921/2835
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 & CVE ID	Patch	NCIIPC ID
within the Bounds of a Memory Buffer			Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile	security/bull etins/august- 2021-bulletin	
			CVE ID : CVE-2021-1930		
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	08-Sep-21	10	Possible buffer overflow due to improper validation of device types during P2P search in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Woice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking CVE ID : CVE-2021-1972	https://www. qualcomm.co m/company/ product- security/bull etins/august- 2021-bulletin	0-QUA-QCA6- 200921/2836
qca6574_firm	iware				
Exposure of Resource to Wrong Sphere	08-Sep-21	2.1	Child process can leak information from parent process due to numeric pids are getting compared and these pid can be reused in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wearables CVE ID : CVE-2021-1904	https://www. qualcomm.co m/company/ product- security/bull etins/august- 2021-bulletin	0-QUA-QCA6- 200921/2837
Loop with Unreachable	08-Sep-21	5	Loop with unreachable exit condition may occur due to	https://www. qualcomm.co	0-QUA-QCA6- 200921/2838

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Exit Condition ('Infinite Loop')			improper handling of unsupported input in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Voice & Music, Snapdragon Wearables CVE ID : CVE-2021-1914	m/company/ product- security/bull etins/august- 2021-bulletin	
Out-of- bounds Write	08-Sep-21	10	Possible buffer underflow due to lack of check for negative indices values when processing user provided input in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Voice & Music, Snapdragon Wearables CVE ID : CVE-2021-1916	https://www. qualcomm.co m/company/ product- security/bull etins/august- 2021-bulletin	0-QUA-QCA6- 200921/2839
Integer Underflow (Wrap or Wraparoun d)	08-Sep-21	10	Integer underflow can occur when the RTCP length is lesser than than the actual blocks present in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Voice & Music, Snapdragon Wearables CVE ID : CVE-2021-1919	https://www. qualcomm.co m/company/ product- security/bull etins/august- 2021-bulletin	0-QUA-QCA6- 200921/2840
Integer	08-Sep-21	10	Integer underflow can occur due to improper handling of	https://www. qualcomm.co	0-QUA-QCA6- 200921/2841

 3-4
 4-5
 5-6
 6-7

 Page 1115 of 1474

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
(Wrap or Wraparoun d)			incoming RTCP packets in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Voice & Music, Snapdragon Wearables CVE ID : CVE-2021-1920	m/company/ product- security/bull etins/august- 2021-bulletin	
Incorrect Type Conversion or Cast	08-Sep-21	4.6	Incorrect pointer argument passed to trusted application TA could result in un- intended memory operations in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Industrial IOT CVE ID : CVE-2021-1923	https://www. qualcomm.co m/company/ product- security/bull etins/august- 2021-bulletin	0-QUA-QCA6- 200921/2842
Improper Restriction of Operations within the Bounds of a Memory Buffer	08-Sep-21	3.6	Possible out of bounds read due to incorrect validation of incoming buffer length in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile CVE ID : CVE-2021-1930	https://www. qualcomm.co m/company/ product- security/bull etins/august- 2021-bulletin	0-QUA-QCA6- 200921/2843
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	08-Sep-21	10	Possible buffer overflow due to improper validation of device types during P2P search in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile,	https://www. qualcomm.co m/company/ product- security/bull etins/august- 2021-bulletin	0-QUA-QCA6- 200921/2844

0-1

1-2

5-6

6-7

7-8

8-9

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID			
			Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking					
			CVE ID : CVE-2021-1972					
qca6584au_f	qca6584au_firmware							
Exposure of Resource to Wrong Sphere	08-Sep-21	2.1	Child process can leak information from parent process due to numeric pids are getting compared and these pid can be reused in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wearables CVE ID : CVE-2021-1904	https://www. qualcomm.co m/company/ product- security/bull etins/august- 2021-bulletin	0-QUA-QCA6- 200921/2845			
Loop with Unreachable Exit Condition ('Infinite Loop')	08-Sep-21	5	Loop with unreachable exit condition may occur due to improper handling of unsupported input in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Voice & Music, Snapdragon Wearables CVE ID : CVE-2021-1914	https://www. qualcomm.co m/company/ product- security/bull etins/august- 2021-bulletin	0-QUA-QCA6- 200921/2846			
Out-of- bounds Write	08-Sep-21	10	Possible buffer underflow due to lack of check for negative indices values when processing user provided	https://www. qualcomm.co m/company/ product-	0-QUA-QCA6- 200921/2847			
CVSS Scoring Sc	cale 0-1	1-2	2-3 3-4 4-5 5-6	6-7 7-8	8-9 9-10			

Page 1117 of 1474

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			input in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Voice & Music, Snapdragon Wearables	security/bull etins/august- 2021-bulletin	
			CVE ID : CVE-2021-1916		
Integer Underflow (Wrap or Wraparoun d)	08-Sep-21	10	Integer underflow can occur when the RTCP length is lesser than than the actual blocks present in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Voice & Music, Snapdragon Wearables CVE ID : CVE-2021-1919	https://www. qualcomm.co m/company/ product- security/bull etins/august- 2021-bulletin	0-QUA-QCA6- 200921/2848
			Integer underflow can occur		
Integer Underflow (Wrap or Wraparoun d)	08-Sep-21	10	due to improper handling of incoming RTCP packets in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Voice & Music, Snapdragon Wearables	https://www. qualcomm.co m/company/ product- security/bull etins/august- 2021-bulletin	0-QUA-QCA6- 200921/2849
Improper			CVE ID : CVE-2021-1920 Possible out of bounds read	https://www.	
Restriction of Operations within the	08-Sep-21	3.6	due to incorrect validation of incoming buffer length in Snapdragon Auto, Snapdragon Compute,	qualcomm.co m/company/ product- security/bull	0-QUA-QCA6- 200921/2850

CVSS Scoring Scale	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9
			Pa	ge 1118 (of 1474				

9-10

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Bounds of a Memory Buffer			Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile	etins/august- 2021-bulletin	
			CVE ID : CVE-2021-1930		
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	08-Sep-21	10	Possible buffer overflow due to improper validation of device types during P2P search in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Woice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking CVE ID : CVE-2021-1972	https://www. qualcomm.co m/company/ product- security/bull etins/august- 2021-bulletin	0-QUA-QCA6- 200921/2851
qca6584_firn	nware				
Exposure of Resource to Wrong Sphere	08-Sep-21	2.1	Child process can leak information from parent process due to numeric pids are getting compared and these pid can be reused in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wearables CVE ID : CVE-2021-1904	https://www. qualcomm.co m/company/ product- security/bull etins/august- 2021-bulletin	0-QUA-QCA6- 200921/2852
Loop with Unreachable Exit	08-Sep-21	5	Loop with unreachable exit condition may occur due to improper handling of	https://www. qualcomm.co m/company/	0-QUA-QCA6- 200921/2853
CVSS Scoring Sc	ale 0-1	1-2	2-3 3-4 4-5 5-6	6-7 7-8	8-9 9-10

Page 1119 of 1474

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Condition ('Infinite Loop')			unsupported input in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Voice & Music, Snapdragon Wearables CVE ID : CVE-2021-1914	product- security/bull etins/august- 2021-bulletin	
Out-of- bounds Write	08-Sep-21	10	Possible buffer underflow due to lack of check for negative indices values when processing user provided input in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Voice & Music, Snapdragon Wearables CVE ID : CVE-2021-1916	https://www. qualcomm.co m/company/ product- security/bull etins/august- 2021-bulletin	O-QUA-QCA6- 200921/2854
Integer Underflow (Wrap or Wraparoun d)	08-Sep-21	10	Integer underflow can occur due to improper handling of incoming RTCP packets in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Voice & Music, Snapdragon Wearables CVE ID : CVE-2021-1920	https://www. qualcomm.co m/company/ product- security/bull etins/august- 2021-bulletin	0-QUA-QCA6- 200921/2855
Buffer Copy without Checking	08-Sep-21	10	Possible buffer overflow due to improper validation of device types during P2P	https://www. qualcomm.co m/company/	0-QUA-QCA6- 200921/2856

CVSS Scoring Scale	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10
Page 1120 of 1474										

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Size of Input ('Classic Buffer Overflow')			search in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking CVE ID : CVE-2021-1972	product- security/bull etins/august- 2021-bulletin	
qca6595au_f	irmware				
Exposure of Resource to Wrong Sphere	08-Sep-21	2.1	Child process can leak information from parent process due to numeric pids are getting compared and these pid can be reused in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables CVE ID : CVE-2021-1904	https://www. qualcomm.co m/company/ product- security/bull etins/august- 2021-bulletin	0-QUA-QCA6- 200921/2857
Loop with Unreachable Exit Condition ('Infinite Loop')	08-Sep-21	5	Loop with unreachable exit condition may occur due to improper handling of unsupported input in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Voice & Music, Snapdragon	https://www. qualcomm.co m/company/ product- security/bull etins/august- 2021-bulletin	0-QUA-QCA6- 200921/2858

 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
			Wearables		
			CVE ID : CVE-2021-1914		
Out-of- bounds Write	08-Sep-21	10	Possible buffer underflow due to lack of check for negative indices values when processing user provided input in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Voice & Music, Snapdragon Wearables	https://www. qualcomm.co m/company/ product- security/bull etins/august- 2021-bulletin	0-QUA-QCA6- 200921/2859
			CVE ID : CVE-2021-1916		
Integer Underflow (Wrap or Wraparoun d)	08-Sep-21	10	Integer underflow can occur when the RTCP length is lesser than than the actual blocks present in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Voice & Music, Snapdragon Wearables CVE ID : CVE-2021-1919	https://www. qualcomm.co m/company/ product- security/bull etins/august- 2021-bulletin	0-QUA-QCA6- 200921/2860
Integer Underflow (Wrap or Wraparoun d)	08-Sep-21	10	Integer underflow can occur due to improper handling of incoming RTCP packets in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Voice & Music, Snapdragon Wearables	https://www. qualcomm.co m/company/ product- security/bull etins/august- 2021-bulletin	0-QUA-QCA6- 200921/2861
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 & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2021-1920		
Incorrect Type Conversion or Cast	08-Sep-21	4.6	Incorrect pointer argument passed to trusted application TA could result in un- intended memory operations in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Industrial IOT CVE ID : CVE-2021-1923	https://www. qualcomm.co m/company/ product- security/bull etins/august- 2021-bulletin	0-QUA-QCA6- 200921/2862
Exposure of Resource to Wrong Sphere	08-Sep-21	2.1	Lack of strict validation of bootmode can lead to information disclosure in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wearables CVE ID : CVE-2021-1929	https://www. qualcomm.co m/company/ product- security/bull etins/august- 2021-bulletin	0-QUA-QCA6- 200921/2863
Improper Restriction of Operations within the Bounds of a Memory Buffer	08-Sep-21	3.6	Possible out of bounds read due to incorrect validation of incoming buffer length in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile CVE ID : CVE-2021-1930	https://www. qualcomm.co m/company/ product- security/bull etins/august- 2021-bulletin	0-QUA-QCA6- 200921/2864
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	08-Sep-21	10	Possible buffer overflow due to improper validation of device types during P2P search in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT,	https://www. qualcomm.co m/company/ product- security/bull etins/august- 2021-bulletin	0-QUA-QCA6- 200921/2865

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking		
			CVE ID : CVE-2021-1972		
qca6595_firn	iware				
Exposure of Resource to Wrong Sphere	08-Sep-21	2.1	Child process can leak information from parent process due to numeric pids are getting compared and these pid can be reused in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wearables CVE ID : CVE-2021-1904	https://www. qualcomm.co m/company/ product- security/bull etins/august- 2021-bulletin	0-QUA-QCA6- 200921/2866
Incorrect Type Conversion or Cast	08-Sep-21	4.6	Incorrect pointer argument passed to trusted application TA could result in un- intended memory operations in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Industrial IOT CVE ID : CVE-2021-1923	https://www. qualcomm.co m/company/ product- security/bull etins/august- 2021-bulletin	0-QUA-QCA6- 200921/2867
Exposure of Resource to Wrong Sphere	08-Sep-21	2.1	Lack of strict validation of bootmode can lead to information disclosure in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity,	https://www. qualcomm.co m/company/ product- security/bull etins/august-	0-QUA-QCA6- 200921/2868
CVSS Scoring Sc	ale 0-1	1-2	2-3 3-4 4-5 5-6	6-7 7-8	8-9 9-10

 3-4
 4-5
 5-6
 6-7

 Page 1124 of 1474

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wearables	2021-bulletin	
			CVE ID : CVE-2021-1929		
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	08-Sep-21	10	Possible buffer overflow due to improper validation of device types during P2P search in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Woice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking CVE ID : CVE-2021-1972	https://www. qualcomm.co m/company/ product- security/bull etins/august- 2021-bulletin	0-QUA-QCA6- 200921/2869
qca6694au_f	irmware				
Loop with Unreachable Exit Condition ('Infinite Loop')	08-Sep-21	5	Loop with unreachable exit condition may occur due to improper handling of unsupported input in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Voice & Music, Snapdragon Wearables CVE ID : CVE-2021-1914	https://www. qualcomm.co m/company/ product- security/bull etins/august- 2021-bulletin	0-QUA-QCA6- 200921/2870
Out-of- bounds Write	08-Sep-21	10	Possible buffer underflow due to lack of check for negative indices values when processing user provided	https://www. qualcomm.co m/company/ product-	0-QUA-QCA6- 200921/2871
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 & CVE ID	Patch	NCIIPC ID	
			input in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Voice & Music, Snapdragon Wearables CVE ID : CVE-2021-1916	security/bull etins/august- 2021-bulletin		
Integer Underflow (Wrap or Wraparoun d)	08-Sep-21	10	Integer underflow can occur when the RTCP length is lesser than than the actual blocks present in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Voice & Music, Snapdragon Wearables CVE ID : CVE-2021-1919	https://www. qualcomm.co m/company/ product- security/bull etins/august- 2021-bulletin	0-QUA-QCA6- 200921/2872	
Integer Underflow (Wrap or Wraparoun d)	08-Sep-21	10	Integer underflow can occur due to improper handling of incoming RTCP packets in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Voice & Music, Snapdragon Wearables CVE ID : CVE-2021-1920	https://www. qualcomm.co m/company/ product- security/bull etins/august- 2021-bulletin	0-QUA-QCA6- 200921/2873	
qca6694_firmware						
Loop with Unreachable Exit Condition	08-Sep-21	5	Loop with unreachable exit condition may occur due to improper handling of unsupported input in	https://www. qualcomm.co m/company/ product-	0-QUA-QCA6- 200921/2874	
CVSS Scoring Sc	ale 0-1	1-2	2-3 3-4 4-5 5-6	6-7 7-8	8-9 9-10	

Page 1126 of 1474

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
('Infinite Loop')			Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Voice & Music, Snapdragon Wearables CVE ID : CVE-2021-1914	security/bull etins/august- 2021-bulletin	
Out-of- bounds Write	08-Sep-21	10	Possible buffer underflow due to lack of check for negative indices values when processing user provided input in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Voice & Music, Snapdragon Wearables CVE ID : CVE-2021-1916	https://www. qualcomm.co m/company/ product- security/bull etins/august- 2021-bulletin	0-QUA-QCA6- 200921/2875
Integer Underflow (Wrap or Wraparoun d)	08-Sep-21	10	Integer underflow can occur when the RTCP length is lesser than than the actual blocks present in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Voice & Music, Snapdragon Wearables CVE ID : CVE-2021-1919	https://www. qualcomm.co m/company/ product- security/bull etins/august- 2021-bulletin	0-QUA-QCA6- 200921/2876
Integer Underflow (Wrap or Wraparoun	08-Sep-21	10	Integer underflow can occur due to improper handling of incoming RTCP packets in Snapdragon Auto,	https://www. qualcomm.co m/company/ product-	0-QUA-QCA6- 200921/2877

CVSS Scoring Scale	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10
			D -	1127	- 6 1 1 7 1					

d)			Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Voice & Music, Snapdragon Wearables CVE ID : CVE-2021-1920	security/bull etins/august- 2021-bulletin	
Out-of- bounds Read	08-Sep-21	3.6	Buffer over read could occur due to incorrect check of buffer size while flashing emmc devices in Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking CVE ID : CVE-2021-1928	https://www. qualcomm.co m/company/ product- security/bull etins/august- 2021-bulletin	0-QUA-QCA6- 200921/2878
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	08-Sep-21	10	Possible buffer overflow due to improper validation of device types during P2P search in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Industrial IOT, Snapdragon Woile, Snapdragon Woice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking CVE ID : CVE-2021-1972	https://www. qualcomm.co m/company/ product- security/bull etins/august- 2021-bulletin	0-QUA-QCA6- 200921/2879
qca6696_firm	iware			I	
Exposure of	08-Sep-21	2.1	Child process can leak	https://www.	0-QUA-QCA6-

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Resource to Wrong Sphere			information from parent process due to numeric pids are getting compared and these pid can be reused in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wearables CVE ID : CVE-2021-1904	qualcomm.co m/company/ product- security/bull etins/august- 2021-bulletin	200921/2880
Loop with Unreachable Exit Condition ('Infinite Loop')	08-Sep-21	5	Loop with unreachable exit condition may occur due to improper handling of unsupported input in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Voice & Music, Snapdragon Wearables CVE ID : CVE-2021-1914	https://www. qualcomm.co m/company/ product- security/bull etins/august- 2021-bulletin	0-QUA-QCA6- 200921/2881
Out-of- bounds Write	08-Sep-21	10	Possible buffer underflow due to lack of check for negative indices values when processing user provided input in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Voice & Music, Snapdragon Wearables	https://www. qualcomm.co m/company/ product- security/bull etins/august- 2021-bulletin	0-QUA-QCA6- 200921/2882

CVSS Scoring Scale	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10
Page 1129 of 1474										

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2021-1916		
Integer Underflow (Wrap or Wraparoun d)	08-Sep-21	10	Integer underflow can occur when the RTCP length is lesser than than the actual blocks present in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Voice & Music, Snapdragon Wearables CVE ID : CVE-2021-1919	https://www. qualcomm.co m/company/ product- security/bull etins/august- 2021-bulletin	0-QUA-QCA6- 200921/2883
Integer Underflow (Wrap or Wraparoun d)	08-Sep-21	10	Integer underflow can occur due to improper handling of incoming RTCP packets in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Voice & Music, Snapdragon Wearables CVE ID : CVE-2021-1920	https://www. qualcomm.co m/company/ product- security/bull etins/august- 2021-bulletin	0-QUA-QCA6- 200921/2884
Incorrect Type Conversion or Cast	08-Sep-21	4.6	Incorrect pointer argument passed to trusted application TA could result in un- intended memory operations in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Industrial IOT CVE ID : CVE-2021-1923	https://www. qualcomm.co m/company/ product- security/bull etins/august- 2021-bulletin	0-QUA-QCA6- 200921/2885
Exposure of Resource to Wrong Sphere CVSS Scoring Sc	08-Sep-21 ale 0-1	2.1	Lack of strict validation of bootmode can lead to information disclosure in Snapdragon Auto, 2-3 3-4 4-5 5-6	https://www. qualcomm.co m/company/ product-	0-QUA-QCA6- 200921/2886 8-9 9-10

Page 1130 of 1474

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID	
			Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wearables	security/bull etins/august- 2021-bulletin		
			CVE ID : CVE-2021-1929			
Improper Restriction of Operations within the Bounds of a Memory Buffer	08-Sep-21	3.6	Possible out of bounds read due to incorrect validation of incoming buffer length in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile CVE ID : CVE-2021-1930	https://www. qualcomm.co m/company/ product- security/bull etins/august- 2021-bulletin	0-QUA-QCA6- 200921/2887	
			Possible buffer overflow due			
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')		10	to improper validation of device types during P2P search in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Woice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking CVE ID : CVE-2021-1972	https://www. qualcomm.co m/company/ product- security/bull etins/august- 2021-bulletin	0-QUA-QCA6- 200921/2888	
qca7500_firmware						
Out-of- bounds Read	08-Sep-21	3.6	Buffer over read could occur due to incorrect check of buffer size while flashing emmc devices in Snapdragon Connectivity, Snapdragon	https://www. qualcomm.co m/company/ product- security/bull	0-QUA-QCA7- 200921/2889	
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 & CVE ID	Patch	NCIIPC ID
			Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking	etins/august- 2021-bulletin	
			CVE ID : CVE-2021-1928		
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	08-Sep-21	10	Possible buffer overflow due to improper validation of device types during P2P search in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Woice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking CVE ID : CVE-2021-1972	https://www. qualcomm.co m/company/ product- security/bull etins/august- 2021-bulletin	O-QUA-QCA7- 200921/2890
qca7520_firm	nware			L	
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	08-Sep-21	10	Possible buffer overflow due to improper validation of device types during P2P search in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Woice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking	https://www. qualcomm.co m/company/ product- security/bull etins/august- 2021-bulletin	0-QUA-QCA7- 200921/2891

CVSS Scoring Scale	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10
Page 1132 of 1474										

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2021-1972		
qca7550_firm	nware				
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	08-Sep-21	10	Possible buffer overflow due to improper validation of device types during P2P search in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Woice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking CVE ID : CVE-2021-1972	https://www. qualcomm.co m/company/ product- security/bull etins/august- 2021-bulletin	O-QUA-QCA7- 200921/2892
qca8072_firm	nware			L	I
Out-of- bounds Read	08-Sep-21	3.6	Buffer over read could occur due to incorrect check of buffer size while flashing emmc devices in Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking CVE ID : CVE-2021-1928	https://www. qualcomm.co m/company/ product- security/bull etins/august- 2021-bulletin	0-QUA-QCA8- 200921/2893
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	08-Sep-21	10	Possible buffer overflow due to improper validation of device types during P2P search in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT,	https://www. qualcomm.co m/company/ product- security/bull etins/august- 2021-bulletin	0-QUA-QCA8- 200921/2894
CVSS Scoring Sc	ale 0-1	1-2	2-3 3-4 4-5 5-6 Page 1133 of 1474	6-7 7-8	8-9 9-10

Page 1133 of 1474

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking CVE ID : CVE-2021-1972		
qca8075_firm	nware				
Out-of- bounds Read	08-Sep-21	3.6	Buffer over read could occur due to incorrect check of buffer size while flashing emmc devices in Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking CVE ID : CVE-2021-1928	https://www. qualcomm.co m/company/ product- security/bull etins/august- 2021-bulletin	0-QUA-QCA8- 200921/2895
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	08-Sep-21	10	Possible buffer overflow due to improper validation of device types during P2P search in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Industrial IOT, Snapdragon Woile, Snapdragon Woice & Music, Snapdragon Wired Infrastructure and Networking CVE ID : CVE-2021-1972	https://www. qualcomm.co m/company/ product- security/bull etins/august- 2021-bulletin	0-QUA-QCA8- 200921/2896
qca8081_firm	nware				
CVSS Scoring Sc	ale 0-1	1-2	2-3 3-4 4-5 5-6	6-7 7-8	8-9 9-10

			Buffer over read could occur		
Out-of- bounds Read	08-Sep-21	3.6	due to incorrect check of buffer size while flashing emmc devices in Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking	https://www. qualcomm.co m/company/ product- security/bull etins/august- 2021-bulletin	0-QUA-QCA8- 200921/2897
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	08-Sep-21	10	CVE ID : CVE-2021-1928 Possible buffer overflow due to improper validation of device types during P2P search in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Industrial IOT, Snapdragon Woile, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking CVE ID : CVE-2021-1972	https://www. qualcomm.co m/company/ product- security/bull etins/august- 2021-bulletin	0-QUA-QCA8- 200921/2898
qca8337_firm	nware				
Exposure of Resource to Wrong Sphere	08-Sep-21	2.1	Child process can leak information from parent process due to numeric pids are getting compared and these pid can be reused in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT,	https://www. qualcomm.co m/company/ product- security/bull etins/august- 2021-bulletin	0-QUA-QCA8- 200921/2899

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables		
			CVE ID : CVE-2021-1904		
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	08-Sep-21	10	Possible buffer overflow due to improper validation of device types during P2P search in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Woice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking CVE ID : CVE-2021-1972	https://www. qualcomm.co m/company/ product- security/bull etins/august- 2021-bulletin	0-QUA-QCA8- 200921/2900
qca9367_firm	nware				
Exposure of Resource to Wrong Sphere	08-Sep-21	2.1	Child process can leak information from parent process due to numeric pids are getting compared and these pid can be reused in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wearables CVE ID : CVE-2021-1904	https://www. qualcomm.co m/company/ product- security/bull etins/august- 2021-bulletin	0-QUA-QCA9- 200921/2901
Loop with Unreachable Exit Condition	08-Sep-21	5	Loop with unreachable exit condition may occur due to improper handling of unsupported input in	https://www. qualcomm.co m/company/ product-	0-QUA-QCA9- 200921/2902
CVSS Scoring Sc	ale 0-1	1-2	2-3 3-4 4-5 5-6	6-7 7-8	8-9 9-10

Page 1136 of 1474

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
('Infinite Loop')			Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Voice & Music, Snapdragon Wearables	security/bull etins/august- 2021-bulletin	
Out-of- bounds Write	08-Sep-21	10	CVE ID : CVE-2021-1914 Possible buffer underflow due to lack of check for negative indices values when processing user provided input in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Voice & Music, Snapdragon Wearables CVE ID : CVE-2021-1916	https://www. qualcomm.co m/company/ product- security/bull etins/august- 2021-bulletin	0-QUA-QCA9- 200921/2903
Integer Underflow (Wrap or Wraparoun d)	08-Sep-21	10	Integer underflow can occur when the RTCP length is lesser than than the actual blocks present in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Voice & Music, Snapdragon Wearables CVE ID : CVE-2021-1919	https://www. qualcomm.co m/company/ product- security/bull etins/august- 2021-bulletin	0-QUA-QCA9- 200921/2904
Integer Underflow (Wrap or Wraparoun	08-Sep-21	10	Integer underflow can occur due to improper handling of incoming RTCP packets in Snapdragon Auto,	https://www. qualcomm.co m/company/ product-	0-QUA-QCA9- 200921/2905

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
d)			Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Voice & Music, Snapdragon Wearables CVE ID : CVE-2021-1920	security/bull etins/august- 2021-bulletin	
Out-of- bounds Read	08-Sep-21	3.6	Buffer over read could occur due to incorrect check of buffer size while flashing emmc devices in Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking CVE ID : CVE-2021-1928	https://www. qualcomm.co m/company/ product- security/bull etins/august- 2021-bulletin	0-QUA-QCA9- 200921/2906
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	08-Sep-21	10	Possible buffer overflow due to improper validation of device types during P2P search in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Industrial IOT, Snapdragon Woile, Snapdragon Woice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking CVE ID : CVE-2021-1972	https://www. qualcomm.co m/company/ product- security/bull etins/august- 2021-bulletin	0-QUA-QCA9- 200921/2907
qca9377_firm	nware				
Exposure of	08-Sep-21	2.1	Child process can leak	https://www.	0-QUA-QCA9-
CVSS Scoring Sc	ale 0-1	1-2	2-3 3-4 4-5 5-6 Page 1138 of 1474	6-7 7-8	8-9 <mark>9-10</mark>

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Resource to Wrong Sphere			information from parent process due to numeric pids are getting compared and these pid can be reused in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wearables CVE ID : CVE-2021-1904	qualcomm.co m/company/ product- security/bull etins/august- 2021-bulletin	200921/2908
Loop with Unreachable Exit Condition ('Infinite Loop')	08-Sep-21	5	Loop with unreachable exit condition may occur due to improper handling of unsupported input in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Voice & Music, Snapdragon Wearables CVE ID : CVE-2021-1914	https://www. qualcomm.co m/company/ product- security/bull etins/august- 2021-bulletin	0-QUA-QCA9- 200921/2909
Out-of- bounds Write	08-Sep-21	10	Possible buffer underflow due to lack of check for negative indices values when processing user provided input in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Voice & Music, Snapdragon Wearables	https://www. qualcomm.co m/company/ product- security/bull etins/august- 2021-bulletin	0-QUA-QCA9- 200921/2910

CVSS Scoring Scale	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10
Page 1139 of 1474										

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2021-1916		
Integer Underflow (Wrap or Wraparoun d)	08-Sep-21	10	Integer underflow can occur when the RTCP length is lesser than than the actual blocks present in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Voice & Music, Snapdragon Wearables CVE ID : CVE-2021-1919	https://www. qualcomm.co m/company/ product- security/bull etins/august- 2021-bulletin	0-QUA-QCA9- 200921/2911
Integer Underflow (Wrap or Wraparoun d)	08-Sep-21	10	Integer underflow can occur due to improper handling of incoming RTCP packets in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Voice & Music, Snapdragon Wearables CVE ID : CVE-2021-1920	https://www. qualcomm.co m/company/ product- security/bull etins/august- 2021-bulletin	O-QUA-QCA9- 200921/2912
Out-of- bounds Read	08-Sep-21	3.6	Buffer over read could occur due to incorrect check of buffer size while flashing emmc devices in Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking CVE ID : CVE-2021-1928	https://www. qualcomm.co m/company/ product- security/bull etins/august- 2021-bulletin	0-QUA-QCA9- 200921/2913

 3-4
 4-5
 5-6
 6-7

 Page 1140 of 1474

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Improper Restriction of Operations within the Bounds of a Memory Buffer	08-Sep-21	3.6	Possible out of bounds read due to incorrect validation of incoming buffer length in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile CVE ID : CVE-2021-1930	https://www. qualcomm.co m/company/ product- security/bull etins/august- 2021-bulletin	0-QUA-QCA9- 200921/2914
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	08-Sep-21	10	Possible buffer overflow due to improper validation of device types during P2P search in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Woice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking CVE ID : CVE-2021-1972	https://www. qualcomm.co m/company/ product- security/bull etins/august- 2021-bulletin	O-QUA-QCA9- 200921/2915
qca9379_firm	nware				
Exposure of Resource to Wrong Sphere	08-Sep-21	2.1	Child process can leak information from parent process due to numeric pids are getting compared and these pid can be reused in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music,	https://www. qualcomm.co m/company/ product- security/bull etins/august- 2021-bulletin	O-QUA-QCA9- 200921/2916

CVSS Scoring Scale	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10	
Page 1141 of 1474											

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Snapdragon Wearables		
			CVE ID : CVE-2021-1904		
Loop with Unreachable Exit Condition ('Infinite Loop')	08-Sep-21	5	Loop with unreachable exit condition may occur due to improper handling of unsupported input in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Voice & Music, Snapdragon Wearables	https://www. qualcomm.co m/company/ product- security/bull etins/august- 2021-bulletin	O-QUA-QCA9- 200921/2917
			CVE ID : CVE-2021-1914		
Out-of- bounds Write	08-Sep-21	10	Possible buffer underflow due to lack of check for negative indices values when processing user provided input in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Voice & Music, Snapdragon Wearables	https://www. qualcomm.co m/company/ product- security/bull etins/august- 2021-bulletin	0-QUA-QCA9- 200921/2918
			CVE ID : CVE-2021-1916		
Integer Underflow (Wrap or Wraparoun d)	08-Sep-21	10	Integer underflow can occur when the RTCP length is lesser than than the actual blocks present in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Voice & Music, Snapdragon	https://www. qualcomm.co m/company/ product- security/bull etins/august- 2021-bulletin	O-QUA-QCA9- 200921/2919

CVSS Scoring Scale

0-1

1-2

3-4 2-3 Page 1142 of 1474

4-5

5-6

6-7

7-8

8-9

9-10

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Wearables		
			CVE ID : CVE-2021-1919		
Integer Underflow (Wrap or Wraparoun d)	08-Sep-21	10	Integer underflow can occur due to improper handling of incoming RTCP packets in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Voice & Music, Snapdragon Wearables	https://www. qualcomm.co m/company/ product- security/bull etins/august- 2021-bulletin	0-QUA-QCA9- 200921/2920
			CVE ID : CVE-2021-1920		
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	08-Sep-21	10	Possible buffer overflow due to improper validation of device types during P2P search in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Woice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking CVE ID : CVE-2021-1972	https://www. qualcomm.co m/company/ product- security/bull etins/august- 2021-bulletin	0-QUA-QCA9- 200921/2921
qca9531_firm	nware				
Out-of- bounds Read	08-Sep-21	3.6	Buffer over read could occur due to incorrect check of buffer size while flashing emmc devices in Snapdragon Connectivity, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice &	https://www. qualcomm.co m/company/ product- security/bull etins/august- 2021-bulletin	0-QUA-QCA9- 200921/2922
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 & CVE ID	Patch	NCIIPC ID
			Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking		
			CVE ID : CVE-2021-1928		
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	08-Sep-21	10	Possible buffer overflow due to improper validation of device types during P2P search in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Woice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking CVE ID : CVE-2021-1972	https://www. qualcomm.co m/company/ product- security/bull etins/august- 2021-bulletin	0-QUA-QCA9- 200921/2923
qca9558_firm	nware				
Out-of- bounds Read	08-Sep-21	3.6	Buffer over read could occur due to incorrect check of buffer size while flashing emmc devices in Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking CVE ID : CVE-2021-1928	https://www. qualcomm.co m/company/ product- security/bull etins/august- 2021-bulletin	0-QUA-QCA9- 200921/2924
Buffer Copy without Checking Size of Input	08-Sep-21	10	Possible buffer overflow due to improper validation of device types during P2P search in Snapdragon Auto,	https://www. qualcomm.co m/company/ product-	0-QUA-QCA9- 200921/2925
CVSS Scoring Sc	ale 0-1	1-2	2-3 3-4 4-5 5-6	6-7 7-8	8-9 9-10

Page 1144 of 1474

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
('Classic Buffer Overflow')			Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking CVE ID : CVE-2021-1972	security/bull etins/august- 2021-bulletin	
qca9561_firm	nware				
Out-of- bounds Read	08-Sep-21	3.6	Buffer over read could occur due to incorrect check of buffer size while flashing emmc devices in Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking CVE ID : CVE-2021-1928	https://www. qualcomm.co m/company/ product- security/bull etins/august- 2021-bulletin	0-QUA-QCA9- 200921/2926
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	08-Sep-21	10	Possible buffer overflow due to improper validation of device types during P2P search in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Woice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and	https://www. qualcomm.co m/company/ product- security/bull etins/august- 2021-bulletin	0-QUA-QCA9- 200921/2927

CVSS Scoring Scale	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-1
Page 1145 of 1474										

			Patch	NCIIPC ID		
		Networking				
		CVE ID : CVE-2021-1972				
nware						
08-Sep-21	3.6	Buffer over read could occur due to incorrect check of buffer size while flashing emmc devices in Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking CVE ID : CVE-2021-1928	https://www. qualcomm.co m/company/ product- security/bull etins/august- 2021-bulletin	0-QUA-QCA9- 200921/2928		
08-Sep-21	10	Possible buffer overflow due to improper validation of device types during P2P search in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Woice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking CVE ID : CVE-2021-1972	https://www. qualcomm.co m/company/ product- security/bull etins/august- 2021-bulletin	0-QUA-QCA9- 200921/2929		
qca9880_firmware						
08-Sep-21	3.6	Buffer over read could occur due to incorrect check of buffer size while flashing emmc devices in Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon	https://www. qualcomm.co m/company/ product- security/bull etins/august-	0-QUA-QCA9- 200921/2930		
	08-Sep-21 08-Sep-21	08-Sep-21 3.6 08-Sep-21 10 08-Sep-21 3.6	OPENDECVE ID : CVE-2021-1972Image: CVE ID : CVE-2021-1972Buffer over read could occur due to incorrect check of buffer size while flashing emmc devices in Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wired Infrastructure and Networking08-Sep-21Image: CVE ID : CVE-2021-192808-Sep-21Image: CVE ID : CVE-2021-1928 Action of tevice types during P2P search in Snapdragon Auto, Snapdragon Conpute, Snapdragon Compute, Snapdragon Compute, Snapdragon Consumer IOT, Snapdragon Consumer IOT, Snapdragon Consumer IOT, Snapdragon Mobile, Snapdragon Noice & Music, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wired Infrastructure and Networking08-Sep-21Image: CVE ID : CVE-2021-197208-Sep-21Image: CVE ID : CVE-2021-197208-Sep-21Suffer over read could occur due to incorrect check of Networking08-Sep-21Saffer over read could occur due to incorrect check of Networking08-Sep-21Saffer over read could occur due to incorrect check of Snapdragon Wired Infrastructure and Networking08-Sep-21Saffer over read could occur due to incorrect check of Suffer size while flashing emmc devices in Snapdragon Connectivity, Snapdragon <b< td=""><td>ImageCVE ID : CVE-2021-1972ImageBuffer over read could occur due to incorrect check of buffer size while flashing emmc devices in Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Networkinghttps://www. qualcomm.co m/company/ product- search in Snapdragon Connectivity, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Nobile, Snapdragon Wired Infrastructure and Networking CVE ID : CVE-2021-1972https://www. qualcomm.co m/company/ product- security/bull etins/august- 2021-bulletin08-Sep-213.6Buffer over read could occur due to incorrect check of buffer size while flashing emmc devices in Snapdragon Connectivity, Snapdragon Connectivity, Snapdragon Connectivity, Snapdragon product- security/bull etins/august- 2021-bulletin08-Sep-213.6Buffer over read could occur due to incorrect check of buffer size while flashing emmc devices in Snapdragon Connectivity, Snapdragon Connectivity, Snapdragon Connectivity, Snapdragonhttps://www. qualcomm.co m/company/ product- security/bull etins/august-08</td></b<>	ImageCVE ID : CVE-2021-1972ImageBuffer over read could occur due to incorrect check of buffer size while flashing emmc devices in Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Networkinghttps://www. qualcomm.co m/company/ product- search in Snapdragon Connectivity, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Nobile, Snapdragon Wired Infrastructure and Networking CVE ID : CVE-2021-1972https://www. qualcomm.co m/company/ product- security/bull etins/august- 2021-bulletin08-Sep-213.6Buffer over read could occur due to incorrect check of buffer size while flashing emmc devices in Snapdragon Connectivity, Snapdragon Connectivity, Snapdragon Connectivity, Snapdragon product- security/bull etins/august- 2021-bulletin08-Sep-213.6Buffer over read could occur due to incorrect check of buffer size while flashing emmc devices in Snapdragon Connectivity, Snapdragon Connectivity, Snapdragon Connectivity, Snapdragonhttps://www. qualcomm.co m/company/ product- security/bull etins/august-08		

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking	2021-bulletin	
			CVE ID : CVE-2021-1928		
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	08-Sep-21	10	Possible buffer overflow due to improper validation of device types during P2P search in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Woice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking CVE ID : CVE-2021-1972	https://www. qualcomm.co m/company/ product- security/bull etins/august- 2021-bulletin	0-QUA-QCA9- 200921/2931
qca9882_firm	nware				
Out-of- bounds Read	08-Sep-21	3.6	Buffer over read could occur due to incorrect check of buffer size while flashing emmc devices in Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking CVE ID : CVE-2021-1928	https://www. qualcomm.co m/company/ product- security/bull etins/august- 2021-bulletin	0-QUA-QCA9- 200921/2932
Buffer Copy without	08-Sep-21	10	Possible buffer overflow due to improper validation of	https://www. qualcomm.co	0-QUA-QCA9- 200921/2933

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Checking Size of Input ('Classic Buffer Overflow')			device types during P2P search in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Woice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking CVE ID : CVE-2021-1972	m/company/ product- security/bull etins/august- 2021-bulletin	
qca9886_firm	nware				
Out-of- bounds Read	08-Sep-21	3.6	Buffer over read could occur due to incorrect check of buffer size while flashing emmc devices in Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking CVE ID : CVE-2021-1928	https://www. qualcomm.co m/company/ product- security/bull etins/august- 2021-bulletin	0-QUA-QCA9- 200921/2934
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	08-Sep-21	10	Possible buffer overflow due to improper validation of device types during P2P search in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Woice & Music, Snapdragon Wearables, Snapdragon Wired	https://www. qualcomm.co m/company/ product- security/bull etins/august- 2021-bulletin	0-QUA-QCA9- 200921/2935

Page 1148 of 1474

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID	
			Infrastructure and Networking			
			5			
			CVE ID : CVE-2021-1972			
qca9887_firn	nware			1	1	
Out-of- bounds Read	08-Sep-21	3.6	Buffer over read could occur due to incorrect check of buffer size while flashing emmc devices in Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking CVE ID : CVE-2021-1928	https://www. qualcomm.co m/company/ product- security/bull etins/august- 2021-bulletin	0-QUA-QCA9- 200921/2936	
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	08-Sep-21	10	Possible buffer overflow due to improper validation of device types during P2P search in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Woice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking CVE ID : CVE-2021-1972	https://www. qualcomm.co m/company/ product- security/bull etins/august- 2021-bulletin	0-QUA-QCA9- 200921/2937	
qca9888_firmware						
Out-of- bounds Read	08-Sep-21	3.6	Buffer over read could occur due to incorrect check of buffer size while flashing emmc devices in Snapdragon Connectivity, Snapdragon	https://www. qualcomm.co m/company/ product- security/bull	0-QUA-QCA9- 200921/2938	
CVSS Scoring Sc	ale 0-1	1-2	2-3 3-4 4-5 5-6	6-7 7-8	8-9 <mark>9-10</mark>	

Buffer Copy without (Classic Buffer Overflow')etins/august- august- 2021-bulletinetins/august- 2021-bulletinBuffer Copy without (Classic Buffer Overflow')08-Sep-21No august- 2021-bulletinPossible buffer overflow due to improper validation of device types during P2P search in Snapdragon Mobile, Snapdragon Consumer 107, Snapdragon Consumer 107, Snapdragon Mobile, Snapdragon Onote: (Classic Buffer Overflow')Networkinghttps://www. qualcomm.co m/company/ product- search in Snapdragon Mobile, Snapdragon Onote: Nangdragon Mobile, Snapdragon Wired Infrastructure and Networking CVE D : CVE-2021-1972QUA-QCA9- 20021/2939qca9889_firtwareJuffer Over read could occur due to incorrect check of buffer size while flashing emmc devices in Snapdragon Mobile, Snapdragon Networkinghttps://www. qualcomm.co m/company/ product- security/bullOut-of- bounds Read08-Sep-213.6Buffer Over read could occur due to incorrect check of buffer size while flashing emmc devices in Snapdragon Mobile, Snapdragon Consumer 107, Snapdragon Mobile, Snapdragon Mobile, Snapdragon Security/bullhttps://www. qualcomm.co m/company/ product- security/bull0ut-of- bounds Read08-Sep-213.6Buffer Over read could occur due to incorrect check of buffer size while flashing emmc devices in Snapdragon Mobile, Snapdragon Mobile, Snapdragon Mobile, Snapdragon Wearables, Snapdr	Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')Itsp://www. sapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Mobile, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wied Infrastructure and Networkinghttps://www. qualcomm.co m/company/ product- security/bull etins/august- 201921/2939O-QUA-QCA9- 200921/2939Out-of- Dounds Read08-Sep-21IBuffer over read could occur due to incorrect check of buffer size while flashing industrial IOT, Snapdragon Noite, Snapdragon Voice & Music, Snapdragon Wired Infrastructure and Networkinghttps://www. qualcomm.co m/company/ product- security/bull etins/august- 2021-bulletinO-QUA-QCA9- 200921/2939Out-of- bounds08-Sep-21JBuffer over read could occur due to incorrect check of buffer size while flashing industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Voice & Snapdragon Voice & Snapdragon Voice & Snapdragon Mobile, Snapdragon Mobile, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Voice & Musi				Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking		
Out-of- bounds Read08-Sep-21B. buffer size while flashing emmc devices in Snapdragon Connectivity, Snapdragon Mobile, Snapdragon Mobile, Snapdragon Wired Infrastructure and Networkinghttps://www. qualcomm.co m/company/ product- security/bull etins/august- 2021-bulletin0-QUA-QCA9- 	without Checking Size of Input ('Classic Buffer	08-Sep-21	10	to improper validation of device types during P2P search in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Woice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking	qualcomm.co m/company/ product- security/bull etins/august-	
Out-of- bounds Read08-Sep-213.6due to incorrect check of buffer size while flashing emmc devices in Snapdragon Connectivity, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Mosic, Snapdragon Voice & Security/bull etins/august- 2021-bulletinhttps://www. qualcomm.co m/company/ product- security/bull etins/august- 2021-bulletinO-QUA-QCA9- 200921/2940	qca9889_firm	nware				
Buffer Copy 08-Sep-21 10 Possible buffer overflow due https://www. 0-QUA-QCA9-	bounds	08-Sep-21	3.6	due to incorrect check of buffer size while flashing emmc devices in Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking	qualcomm.co m/company/ product- security/bull etins/august-	• •
	Buffer Copy	08-Sep-21	10	Possible buffer overflow due	https://www.	0-QUA-QCA9-

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
without Checking Size of Input ('Classic Buffer Overflow')			to improper validation of device types during P2P search in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Woice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking	qualcomm.co m/company/ product- security/bull etins/august- 2021-bulletin	200921/2941
			CVE ID : CVE-2021-1972		
qca9896_firn	nware				
Out-of- bounds Read	08-Sep-21	3.6	Buffer over read could occur due to incorrect check of buffer size while flashing emmc devices in Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking CVE ID : CVE-2021-1928	https://www. qualcomm.co m/company/ product- security/bull etins/august- 2021-bulletin	0-QUA-QCA9- 200921/2942
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	08-Sep-21	10	Possible buffer overflow due to improper validation of device types during P2P search in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables,	https://www. qualcomm.co m/company/ product- security/bull etins/august- 2021-bulletin	0-QUA-QCA9- 200921/2943

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID				
			Snapdragon Wired Infrastructure and Networking						
			CVE ID : CVE-2021-1972						
qca9898_firm	qca9898_firmware								
Out-of- bounds Read	08-Sep-21	3.6	Buffer over read could occur due to incorrect check of buffer size while flashing emmc devices in Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking	https://www. qualcomm.co m/company/ product- security/bull etins/august- 2021-bulletin	0-QUA-QCA9- 200921/2944				
			CVE ID : CVE-2021-1928						
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	08-Sep-21	10	Possible buffer overflow due to improper validation of device types during P2P search in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Woice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking CVE ID : CVE-2021-1972	https://www. qualcomm.co m/company/ product- security/bull etins/august- 2021-bulletin	0-QUA-QCA9- 200921/2945				
qca9980_firm	qca9980_firmware								
Out-of- bounds Read	08-Sep-21	3.6	Buffer over read could occur due to incorrect check of buffer size while flashing emmc devices in Snapdragon	https://www. qualcomm.co m/company/ product-	0-QUA-QCA9- 200921/2946				
CVSS Scoring Sc	ale 0-1	1-2	2-3 3-4 4-5 5-6 Page 1152 of 1474	6-7 7-8	8-9 9-10				

Page 1152 of 1474

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking CVE ID : CVE-2021-1928	security/bull etins/august- 2021-bulletin	
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	08-Sep-21	10	Possible buffer overflow due to improper validation of device types during P2P search in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Industrial IOT, Snapdragon Woile, Snapdragon Woice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking CVE ID : CVE-2021-1972	https://www. qualcomm.co m/company/ product- security/bull etins/august- 2021-bulletin	0-QUA-QCA9- 200921/2947
qca9982_firn	nware				
Out-of- bounds Read	08-Sep-21	3.6	Buffer over read could occur due to incorrect check of buffer size while flashing emmc devices in Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking CVE ID : CVE-2021-1928	https://www. qualcomm.co m/company/ product- security/bull etins/august- 2021-bulletin	0-QUA-QCA9- 200921/2948

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	08-Sep-21	10	Possible buffer overflow due to improper validation of device types during P2P search in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Woice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking CVE ID : CVE-2021-1972	https://www. qualcomm.co m/company/ product- security/bull etins/august- 2021-bulletin	0-QUA-QCA9- 200921/2949
qca9984_firm	nware				
Out-of- bounds Read	08-Sep-21	3.6	Buffer over read could occur due to incorrect check of buffer size while flashing emmc devices in Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking CVE ID : CVE-2021-1928	https://www. qualcomm.co m/company/ product- security/bull etins/august- 2021-bulletin	0-QUA-QCA9- 200921/2950
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	08-Sep-21	10	Possible buffer overflow due to improper validation of device types during P2P search in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music,	https://www. qualcomm.co m/company/ product- security/bull etins/august- 2021-bulletin	0-QUA-QCA9- 200921/2951

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking		
			CVE ID : CVE-2021-1972		
qca9985_firm	nware				
Out-of- bounds Read	08-Sep-21	3.6	Buffer over read could occur due to incorrect check of buffer size while flashing emmc devices in Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking	https://www. qualcomm.co m/company/ product- security/bull etins/august- 2021-bulletin	0-QUA-QCA9- 200921/2952
			CVE ID : CVE-2021-1928		
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	08-Sep-21	10	Possible buffer overflow due to improper validation of device types during P2P search in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Woice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking CVE ID : CVE-2021-1972	https://www. qualcomm.co m/company/ product- security/bull etins/august- 2021-bulletin	O-QUA-QCA9- 200921/2953
qca9986_firm	nware				
Buffer Copy without Checking	08-Sep-21	10	Possible buffer overflow due to improper validation of device types during P2P	https://www. qualcomm.co m/company/	0-QUA-QCA9- 200921/2954
CVSS Scoring Sc	ale 0-1	1-2	2-3 3-4 4-5 5-6 Page 1155 of 1474	6-7 7-8	8-9 9-10

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Size of Input ('Classic Buffer Overflow')			search in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking CVE ID : CVE-2021-1972	product- security/bull etins/august- 2021-bulletin	
qca9987_firm	nware				
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	08-Sep-21	10	Possible buffer overflow due to improper validation of device types during P2P search in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Woice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking CVE ID : CVE-2021-1972	https://www. qualcomm.co m/company/ product- security/bull etins/august- 2021-bulletin	O-QUA-QCA9- 200921/2955
qca9988_firm	nware				
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	08-Sep-21	10	Possible buffer overflow due to improper validation of device types during P2P search in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile,	https://www. qualcomm.co m/company/ product- security/bull etins/august- 2021-bulletin	O-QUA-QCA9- 200921/2956

CVSS Scoring Scale 0-1

1-2

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-2021-1972		
qca9990_firn	nware				
Out-of- bounds Read	08-Sep-21	3.6	Buffer over read could occur due to incorrect check of buffer size while flashing emmc devices in Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking CVE ID : CVE-2021-1928	https://www. qualcomm.co m/company/ product- security/bull etins/august- 2021-bulletin	0-QUA-QCA9- 200921/2957
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	08-Sep-21	10	Possible buffer overflow due to improper validation of device types during P2P search in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Woice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking CVE ID : CVE-2021-1972	https://www. qualcomm.co m/company/ product- security/bull etins/august- 2021-bulletin	0-QUA-QCA9- 200921/2958
qca9992_firm	nware				
Out-of- bounds	08-Sep-21	3.6	Buffer over read could occur due to incorrect check of	https://www. qualcomm.co	0-QUA-QCA9-
CVSS Scoring Sc	ale 0-1	1-2	2-3 3-4 4-5 5-6 Page 1157 of 1474	6-7 7-8	8-9 9-10

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Read			buffer size while flashing emmc devices in Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking CVE ID : CVE-2021-1928	m/company/ product- security/bull etins/august- 2021-bulletin	200921/2959
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	08-Sep-21	10	Possible buffer overflow due to improper validation of device types during P2P search in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Woice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking CVE ID : CVE-2021-1972	https://www. qualcomm.co m/company/ product- security/bull etins/august- 2021-bulletin	O-QUA-QCA9- 200921/2960
qca9994_firm	nware				
Out-of- bounds Read	08-Sep-21	3.6	Buffer over read could occur due to incorrect check of buffer size while flashing emmc devices in Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and	https://www. qualcomm.co m/company/ product- security/bull etins/august- 2021-bulletin	O-QUA-QCA9- 200921/2961

CVSS Scoring Scale	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10
			Pa	ge 1158 (of 1474					

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Networking		
			CVE ID : CVE-2021-1928		
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	08-Sep-21	10	Possible buffer overflow due to improper validation of device types during P2P search in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Woice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking CVE ID : CVE-2021-1972	https://www. qualcomm.co m/company/ product- security/bull etins/august- 2021-bulletin	0-QUA-QCA9- 200921/2962
qcm2290_fir	mware				
Exposure of Resource to Wrong Sphere	08-Sep-21	2.1	Child process can leak information from parent process due to numeric pids are getting compared and these pid can be reused in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wearables CVE ID : CVE-2021-1904	https://www. qualcomm.co m/company/ product- security/bull etins/august- 2021-bulletin	0-QUA-QCM2- 200921/2963
Incorrect Type Conversion or Cast	08-Sep-21	4.6	Incorrect pointer argument passed to trusted application TA could result in un- intended memory operations in Snapdragon Auto, Snapdragon Compute,	https://www. qualcomm.co m/company/ product- security/bull etins/august-	0-QUA-QCM2- 200921/2964
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 & CVE ID	Patch	NCIIPC ID
			Snapdragon Connectivity, Snapdragon Industrial IOT CVE ID : CVE-2021-1923	2021-bulletin	
Exposure of Resource to Wrong Sphere	08-Sep-21	2.1	Lack of strict validation of bootmode can lead to information disclosure in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wearables CVE ID : CVE-2021-1929	https://www. qualcomm.co m/company/ product- security/bull etins/august- 2021-bulletin	0-QUA-QCM2- 200921/2965
Improper Restriction of Operations within the Bounds of a Memory Buffer	08-Sep-21	3.6	Possible out of bounds read due to incorrect validation of incoming buffer length in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile CVE ID : CVE-2021-1930	https://www. qualcomm.co m/company/ product- security/bull etins/august- 2021-bulletin	0-QUA-QCM2- 200921/2966
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	08-Sep-21	10	Possible buffer overflow due to improper validation of device types during P2P search in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Woice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking	https://www. qualcomm.co m/company/ product- security/bull etins/august- 2021-bulletin	0-QUA-QCM2- 200921/2967
CVSS Scoring Sco	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-2021-1972		
qcm4290_fir	mware			I	
Exposure of Resource to Wrong Sphere	08-Sep-21	2.1	Child process can leak information from parent process due to numeric pids are getting compared and these pid can be reused in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables CVE ID : CVE-2021-1904	https://www. qualcomm.co m/company/ product- security/bull etins/august- 2021-bulletin	0-QUA-QCM4- 200921/2968
Loop with Unreachable Exit Condition ('Infinite Loop')	08-Sep-21	5	Loop with unreachable exit condition may occur due to improper handling of unsupported input in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Voice & Music, Snapdragon Wearables CVE ID : CVE-2021-1914	https://www. qualcomm.co m/company/ product- security/bull etins/august- 2021-bulletin	0-QUA-QCM4- 200921/2969
Out-of- bounds Write	08-Sep-21	10	Possible buffer underflow due to lack of check for negative indices values when processing user provided input in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT,	https://www. qualcomm.co m/company/ product- security/bull etins/august- 2021-bulletin	0-QUA-QCM4- 200921/2970

CVSS Scoring Scale

0-1

1-2

5-6

6-7

7-8

8-9

9-10

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Snapdragon IoT, Snapdragon Voice & Music, Snapdragon Wearables		
			CVE ID : CVE-2021-1916		
Integer Underflow (Wrap or Wraparoun d)	08-Sep-21	10	Integer underflow can occur when the RTCP length is lesser than than the actual blocks present in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Voice & Music, Snapdragon Wearables CVE ID : CVE-2021-1919	https://www. qualcomm.co m/company/ product- security/bull etins/august- 2021-bulletin	0-QUA-QCM4- 200921/2971
Integer Underflow (Wrap or Wraparoun d)	08-Sep-21	10	Integer underflow can occur due to improper handling of incoming RTCP packets in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Voice & Music, Snapdragon Wearables CVE ID : CVE-2021-1920	https://www. qualcomm.co m/company/ product- security/bull etins/august- 2021-bulletin	O-QUA-QCM4- 200921/2972
Incorrect Type Conversion or Cast	08-Sep-21	4.6	Incorrect pointer argument passed to trusted application TA could result in un- intended memory operations in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Industrial IOT CVE ID : CVE-2021-1923	https://www. qualcomm.co m/company/ product- security/bull etins/august- 2021-bulletin	0-QUA-QCM4- 200921/2973

 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	
Exposure of Resource to Wrong Sphere	08-Sep-21	2.1	Lack of strict validation of bootmode can lead to information disclosure in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wearables CVE ID : CVE-2021-1929	https://www. qualcomm.co m/company/ product- security/bull etins/august- 2021-bulletin	0-QUA-QCM4- 200921/2974	
Improper Restriction of Operations within the Bounds of a Memory Buffer	08-Sep-21	3.6	Possible out of bounds read due to incorrect validation of incoming buffer length in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile CVE ID : CVE-2021-1930	https://www. qualcomm.co m/company/ product- security/bull etins/august- 2021-bulletin	0-QUA-QCM4- 200921/2975	
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	08-Sep-21	10	Possible buffer overflow due to improper validation of device types during P2P search in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Woice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking CVE ID : CVE-2021-1972	https://www. qualcomm.co m/company/ product- security/bull etins/august- 2021-bulletin	O-QUA-QCM4- 200921/2976	
qcm6125_firmware						
Exposure of	08-Sep-21	2.1	Child process can leak	https://www.	0-QUA-QCM6-	
CVSS Scoring Sc	ale 0-1	1-2	2-3 3-4 4-5 5-6 Page 1163 of 1474	6-7 7-8	8-9 9-10	

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Resource to Wrong Sphere			information from parent process due to numeric pids are getting compared and these pid can be reused in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wearables CVE ID : CVE-2021-1904	qualcomm.co m/company/ product- security/bull etins/august- 2021-bulletin	200921/2977
Loop with Unreachable Exit Condition ('Infinite Loop')	08-Sep-21	5	Loop with unreachable exit condition may occur due to improper handling of unsupported input in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Voice & Music, Snapdragon Wearables CVE ID : CVE-2021-1914	https://www. qualcomm.co m/company/ product- security/bull etins/august- 2021-bulletin	0-QUA-QCM6- 200921/2978
Out-of- bounds Write	08-Sep-21	10	Possible buffer underflow due to lack of check for negative indices values when processing user provided input in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Voice & Music, Snapdragon Wearables	https://www. qualcomm.co m/company/ product- security/bull etins/august- 2021-bulletin	0-QUA-QCM6- 200921/2979

CVSS	Scoring Scale	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10
				Pa	age 1164 (of 1474					

Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
		CVE ID : CVE-2021-1916		
08-Sep-21	10	Integer underflow can occur when the RTCP length is lesser than than the actual blocks present in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Voice & Music, Snapdragon Wearables CVE ID : CVE-2021-1919	https://www. qualcomm.co m/company/ product- security/bull etins/august- 2021-bulletin	0-QUA-QCM6- 200921/2980
08-Sep-21	10	Integer underflow can occur due to improper handling of incoming RTCP packets in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Voice & Music, Snapdragon Wearables CVE ID : CVE-2021-1920	https://www. qualcomm.co m/company/ product- security/bull etins/august- 2021-bulletin	0-QUA-QCM6- 200921/2981
08-Sep-21	2.1	Lack of strict validation of bootmode can lead to information disclosure in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wearables CVE ID : CVE-2021-1929	https://www. qualcomm.co m/company/ product- security/bull etins/august- 2021-bulletin	0-QUA-QCM6- 200921/2982
08-Sep-21	3.6	Possible out of bounds read due to incorrect validation of	https://www. qualcomm.co	0-QUA-QCM6- 200921/2983 8-9 9-10
	08-Sep-21 08-Sep-21	Image: marrier of the second secon	Image: constraint of the series of the ser	Image: Note of the second se

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
of Operations within the Bounds of a Memory Buffer			incoming buffer length in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile	m/company/ product- security/bull etins/august- 2021-bulletin	
			CVE ID : CVE-2021-1930		
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	08-Sep-21	10	Possible buffer overflow due to improper validation of device types during P2P search in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Industrial IOT, Snapdragon Woice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking CVE ID : CVE-2021-1972	https://www. qualcomm.co m/company/ product- security/bull etins/august- 2021-bulletin	0-QUA-QCM6- 200921/2984
qcn3018_firr	nware				
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	08-Sep-21	10	Possible buffer overflow due to improper validation of device types during P2P search in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Woice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking	https://www. qualcomm.co m/company/ product- security/bull etins/august- 2021-bulletin	0-QUA-QCN3- 200921/2985

CVSS Scoring Scale	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10
			Dr	000 1166	of 1/17/					

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID		
			CVE ID : CVE-2021-1972				
qcn5021_firmware							
Out-of- bounds Read	08-Sep-21	3.6	Buffer over read could occur due to incorrect check of buffer size while flashing emmc devices in Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking	https://www. qualcomm.co m/company/ product- security/bull etins/august- 2021-bulletin	0-QUA-QCN5- 200921/2986		
			CVE ID : CVE-2021-1928				
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	08-Sep-21	10	Possible buffer overflow due to improper validation of device types during P2P search in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Woice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking CVE ID : CVE-2021-1972	https://www. qualcomm.co m/company/ product- security/bull etins/august- 2021-bulletin	0-QUA-QCN5- 200921/2987		
qcn5022_firm	nware			I	I		
Out-of- bounds Read	08-Sep-21	3.6	Buffer over read could occur due to incorrect check of buffer size while flashing emmc devices in Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon	https://www. qualcomm.co m/company/ product- security/bull etins/august- 2021-bulletin	0-QUA-QCN5- 200921/2988		
CVSS Scoring Sc	ale 0-1	1-2	2-3 3-4 4-5 5-6 Page 1167 of 1474	6-7 7-8	8-9 9-10		

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Mobile, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking		
			CVE ID : CVE-2021-1928		
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	08-Sep-21	10	Possible buffer overflow due to improper validation of device types during P2P search in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Woice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking CVE ID : CVE-2021-1972	https://www. qualcomm.co m/company/ product- security/bull etins/august- 2021-bulletin	0-QUA-QCN5- 200921/2989
qcn5024_firm	nware				
Out-of- bounds Read	08-Sep-21	3.6	Buffer over read could occur due to incorrect check of buffer size while flashing emmc devices in Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking CVE ID : CVE-2021-1928	https://www. qualcomm.co m/company/ product- security/bull etins/august- 2021-bulletin	0-QUA-QCN5- 200921/2990
Buffer Copy without Checking	08-Sep-21	10	Possible buffer overflow due to improper validation of device types during P2P	https://www. qualcomm.co m/company/	0-QUA-QCN5- 200921/2991
CVSS Scoring Sc	ale 0-1	1-2	2-3 3-4 4-5 5-6	6-7 7-8	8-9 9-10

Page 1168 of 1474

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Size of Input ('Classic Buffer Overflow')			search in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking CVE ID : CVE-2021-1972	product- security/bull etins/august- 2021-bulletin	
qcn5052_firm	nware			I	I
Out-of- bounds Read	08-Sep-21	3.6	Buffer over read could occur due to incorrect check of buffer size while flashing emmc devices in Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking CVE ID : CVE-2021-1928	https://www. qualcomm.co m/company/ product- security/bull etins/august- 2021-bulletin	0-QUA-QCN5- 200921/2992
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	08-Sep-21	10	Possible buffer overflow due to improper validation of device types during P2P search in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Woice & Music, Snapdragon Wired Infrastructure and	https://www. qualcomm.co m/company/ product- security/bull etins/august- 2021-bulletin	0-QUA-QCN5- 200921/2993

Page 1169 of 1474

Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
		Networking		
		CVE ID : CVE-2021-1972		
nware				
08-Sep-21	3.6	Buffer over read could occur due to incorrect check of buffer size while flashing emmc devices in Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking CVE ID : CVE-2021-1928	https://www. qualcomm.co m/company/ product- security/bull etins/august- 2021-bulletin	0-QUA-QCN5- 200921/2994
08-Sep-21	10	Possible buffer overflow due to improper validation of device types during P2P search in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Woice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking CVE ID : CVE-2021-1972	https://www. qualcomm.co m/company/ product- security/bull etins/august- 2021-bulletin	0-QUA-QCN5- 200921/2995
nware				
08-Sep-21	3.6	Buffer over read could occur due to incorrect check of buffer size while flashing emmc devices in Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon	https://www. qualcomm.co m/company/ product- security/bull etins/august-	0-QUA-QCN5- 200921/2996
	nware 08-Sep-21 08-Sep-21	oware 08-Sep-21 3.6 08-Sep-21 10 08-Sep-21 10	Image: construct of the second seco	Image: Networking CVE ID : CVE-2021-1972Image: Networking CVE ID : CVE-2021-1972ImwareSuffer over read could occur due to incorrect check of buffer size while flashing emmc devices in Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Voice & Music, Snapdragon Voice & Music, Snapdragon Voice & Music, Snapdragon Verables, Snapdragon Werarables, Snapdragon Werarables, Snapdragon Vere ID : CVE-2021-1928https://www. qualcomm.co m/company/ product- security/bull etins/august- 2021-bulletin08-Sep-2110Possible buffer overflow due to improper validation of device types during P2P search in Snapdragon Auto, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Mobile, Snapdragon Mobile, Snapdragon Mobile, Snapdragon Mobile, Snapdragon Weerables, Snapdragon Wered Infrastructure and Networking CVE ID : CVE-2021-1972https://www. qualcomm.co m/company/ product- security/bull etins/august- 2021-bulletin08-Sep-2110Buffer over read could occur due to incorrect check of buffer size while flashing emmc devices in Snapdragonhttps://www. qualcomm.co m/company/ product- security/bull etins/august- 2021-bulletin08-Sep-213.6Buffer over read could occur due to incorrect check of buffer size while flashing emmc devices in Snapdragonhttps://www. qualcomm.co m/company/ product- security/bull

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking	2021-bulletin	
			CVE ID : CVE-2021-1928		
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	08-Sep-21	10	Possible buffer overflow due to improper validation of device types during P2P search in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Woice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking CVE ID : CVE-2021-1972	https://www. qualcomm.co m/company/ product- security/bull etins/august- 2021-bulletin	0-QUA-QCN5- 200921/2997
qcn5121_firm	nware				
Out-of- bounds Read	08-Sep-21	3.6	Buffer over read could occur due to incorrect check of buffer size while flashing emmc devices in Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking CVE ID : CVE-2021-1928	https://www. qualcomm.co m/company/ product- security/bull etins/august- 2021-bulletin	0-QUA-QCN5- 200921/2998
Buffer Copy without	08-Sep-21	10	Possible buffer overflow due to improper validation of	https://www. qualcomm.co	0-QUA-QCN5- 200921/2999
CVSS Scoring Sc	ale 0-1	1-2	2-3 3-4 4-5 5-6 Page 1171 of 1474	6-7 7-8	8-9 9-10

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Checking Size of Input ('Classic Buffer Overflow')			device types during P2P search in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Woice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking CVE ID : CVE-2021-1972	m/company/ product- security/bull etins/august- 2021-bulletin	
qcn5122_firm	nware				
Out-of- bounds Read	08-Sep-21	3.6	Buffer over read could occur due to incorrect check of buffer size while flashing emmc devices in Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking CVE ID : CVE-2021-1928	https://www. qualcomm.co m/company/ product- security/bull etins/august- 2021-bulletin	0-QUA-QCN5- 200921/3000
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	08-Sep-21	10	Possible buffer overflow due to improper validation of device types during P2P search in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Woice & Music, Snapdragon Wearables, Snapdragon Wired	https://www. qualcomm.co m/company/ product- security/bull etins/august- 2021-bulletin	0-QUA-QCN5- 200921/3001

Page 1172 of 1474

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID				
			Infrastructure and Networking						
			C						
			CVE ID : CVE-2021-1972						
qcn5124_firn	qcn5124_firmware								
Out-of- bounds Read	08-Sep-21	3.6	Buffer over read could occur due to incorrect check of buffer size while flashing emmc devices in Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking CVE ID : CVE-2021-1928	https://www. qualcomm.co m/company/ product- security/bull etins/august- 2021-bulletin	0-QUA-QCN5- 200921/3002				
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	08-Sep-21	10	Possible buffer overflow due to improper validation of device types during P2P search in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Woice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking CVE ID : CVE-2021-1972	https://www. qualcomm.co m/company/ product- security/bull etins/august- 2021-bulletin	0-QUA-QCN5- 200921/3003				
qcn5152_firm	qcn5152_firmware								
Out-of- bounds Read	08-Sep-21	3.6	Buffer over read could occur due to incorrect check of buffer size while flashing emmc devices in Snapdragon Connectivity, Snapdragon	https://www. qualcomm.co m/company/ product- security/bull	0-QUA-QCN5- 200921/3004				
CVSS Scoring Sc	ale 0-1	1-2	2-3 3-4 4-5 5-6 Page 1173 of 1474	6-7 7-8	8-9 9-10				

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking CVE ID : CVE-2021-1928	etins/august- 2021-bulletin	
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	08-Sep-21	10	Possible buffer overflow due to improper validation of device types during P2P search in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Woice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking CVE ID : CVE-2021-1972	https://www. qualcomm.co m/company/ product- security/bull etins/august- 2021-bulletin	0-QUA-QCN5- 200921/3005
qcn5154_firr	nware			<u>I</u>	
Out-of- bounds Read	08-Sep-21	3.6	Buffer over read could occur due to incorrect check of buffer size while flashing emmc devices in Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking CVE ID : CVE-2021-1928	https://www. qualcomm.co m/company/ product- security/bull etins/august- 2021-bulletin	0-QUA-QCN5- 200921/3006
Buffer Copy	08-Sep-21	10	Possible buffer overflow due	https://www.	0-QUA-QCN5-
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 & CVE ID	Patch	NCIIPC ID
without Checking Size of Input ('Classic Buffer Overflow')			to improper validation of device types during P2P search in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Woice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking	qualcomm.co m/company/ product- security/bull etins/august- 2021-bulletin	200921/3007
a an F 1(A finn			CVE ID : CVE-2021-1972		
qcn5164_firm	nware				
Out-of- bounds Read	08-Sep-21	3.6	Buffer over read could occur due to incorrect check of buffer size while flashing emmc devices in Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking CVE ID : CVE-2021-1928	https://www. qualcomm.co m/company/ product- security/bull etins/august- 2021-bulletin	0-QUA-QCN5- 200921/3008
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	08-Sep-21	10	Possible buffer overflow due to improper validation of device types during P2P search in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables,	https://www. qualcomm.co m/company/ product- security/bull etins/august- 2021-bulletin	0-QUA-QCN5- 200921/3009

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Snapdragon Wired Infrastructure and Networking		
			CVE ID : CVE-2021-1972		
qcn5500_firm	nware			Γ	Γ
Out-of- bounds Read	08-Sep-21	3.6	Buffer over read could occur due to incorrect check of buffer size while flashing emmc devices in Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking	https://www. qualcomm.co m/company/ product- security/bull etins/august- 2021-bulletin	0-QUA-QCN5- 200921/3010
			CVE ID : CVE-2021-1928		
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	08-Sep-21	10	Possible buffer overflow due to improper validation of device types during P2P search in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Woice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking CVE ID : CVE-2021-1972	https://www. qualcomm.co m/company/ product- security/bull etins/august- 2021-bulletin	0-QUA-QCN5- 200921/3011
qcn5502_firm	nware			I	I
Out-of- bounds Read	08-Sep-21	3.6	Buffer over read could occur due to incorrect check of buffer size while flashing emmc devices in Snapdragon	https://www. qualcomm.co m/company/ product-	0-QUA-QCN5- 200921/3012
CVSS Scoring Sc	ale 0-1	1-2	2-3 3-4 4-5 5-6 Page 1176 of 1474	6-7 7-8	8-9 9-10

Page 1176 of 1474

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking CVE ID : CVE-2021-1928	security/bull etins/august- 2021-bulletin	
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	08-Sep-21	10	Possible buffer overflow due to improper validation of device types during P2P search in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Industrial IOT, Snapdragon Woile, Snapdragon Woile, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking CVE ID : CVE-2021-1972	https://www. qualcomm.co m/company/ product- security/bull etins/august- 2021-bulletin	0-QUA-QCN5- 200921/3013
qcn5550_firm	nware				
Out-of- bounds Read	08-Sep-21	3.6	Buffer over read could occur due to incorrect check of buffer size while flashing emmc devices in Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking CVE ID : CVE-2021-1928	https://www. qualcomm.co m/company/ product- security/bull etins/august- 2021-bulletin	0-QUA-QCN5- 200921/3014
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 & CVE ID	Patch	NCIIPC ID
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	08-Sep-21	10	Possible buffer overflow due to improper validation of device types during P2P search in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Woice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking CVE ID : CVE-2021-1972	https://www. qualcomm.co m/company/ product- security/bull etins/august- 2021-bulletin	0-QUA-QCN5- 200921/3015
qcn6023_firm	nware				
Out-of- bounds Read	08-Sep-21	3.6	Buffer over read could occur due to incorrect check of buffer size while flashing emmc devices in Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking CVE ID : CVE-2021-1928	https://www. qualcomm.co m/company/ product- security/bull etins/august- 2021-bulletin	0-QUA-QCN6- 200921/3016
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	08-Sep-21	10	Possible buffer overflow due to improper validation of device types during P2P search in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music,	https://www. qualcomm.co m/company/ product- security/bull etins/august- 2021-bulletin	0-QUA-QCN6- 200921/3017

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID		
			Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking				
			CVE ID : CVE-2021-1972				
qcn6024_firm	nware			I	I		
Out-of- bounds Read	08-Sep-21	3.6	Buffer over read could occur due to incorrect check of buffer size while flashing emmc devices in Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking	https://www. qualcomm.co m/company/ product- security/bull etins/august- 2021-bulletin	0-QUA-QCN6- 200921/3018		
			CVE ID : CVE-2021-1928				
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	08-Sep-21	10	Possible buffer overflow due to improper validation of device types during P2P search in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Woice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking CVE ID : CVE-2021-1972	https://www. qualcomm.co m/company/ product- security/bull etins/august- 2021-bulletin	0-QUA-QCN6- 200921/3019		
qcn6122_firmware							
Buffer Copy without Checking	08-Sep-21	10	Possible buffer overflow due to improper validation of device types during P2P	https://www. qualcomm.co m/company/	0-QUA-QCN6- 200921/3020		
CVSS Scoring Sc	cale 0-1	1-2	2-3 3-4 4-5 5-6 Page 1179 of 1474	6-7 7-8	8-9 9-10		

Page 1179 of 1474

Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
		search in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking CVE ID : CVE-2021-1972	product- security/bull etins/august- 2021-bulletin	
nware				
08-Sep-21	3.6	Buffer over read could occur due to incorrect check of buffer size while flashing emmc devices in Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking CVE ID : CVE-2021-1928	https://www. qualcomm.co m/company/ product- security/bull etins/august- 2021-bulletin	0-QUA-QCN9- 200921/3021
08-Sep-21	10	Possible buffer overflow due to improper validation of device types during P2P search in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Woice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and	https://www. qualcomm.co m/company/ product- security/bull etins/august- 2021-bulletin	0-QUA-QCN9- 200921/3022
	nware 08-Sep-21	08-Sep-21 3.6 08-Sep-21 10	Image: Construct of the search in Snapdragon Auto, Snapdragon Compute, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wearables, Snapdragon Wearables, Snapdragon Wired Infrastructure and NetworkingImage: CVE ID : CVE-2021-1972Image: CVE ID : CVE-2021-1973Image: CVE ID : CVE-2021-1928Image: CVE ID : CVE-2021-1928	oresearch in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Mobile, Snapdragon Woire & Music, Snapdragon Wired Infrastructure and Networkingproduct- security/bull etins/august- 2021-bulletinnwareU08-Sep-213.6Buffer over read could occur due to incorrect check of buffer size while flashing emmc devices in Snapdragon Consumer IOT, Snapdragon Consumer IOT, Snapdragon Consumer IOT, Snapdragon Mobile, Snapdragon Ocnectivity, Snapdragon Consumer IOT, Snapdragon Music, Snapdragon Vired Infrastructure and Networkinghttps://www. qualcomm.co m/company/ product- security/bull etins/august- 2021-bulletin08-Sep-2110Possible buffer overflow due to improper validation of device types during P2P search in Snapdragon Connectivity, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Consumer IOT, Snapdragon Mobile, Snapdragon Wired Infrastructure and Networkinghttps://www. qualcomm.co m/company/ product- security/bull etins/august- 2021-bulletin08-Sep-2110Possible buffer overflow due to improper validation of device types during P2P search in Snapdragon Auto, Snapdragon Consumer IOT, Snapdragon Consumer IOT, Snapdragon Consumer IOT, Snapdragon Mobile, Snapdragon Consumer IOT, Snapdragon Consumer IOT, Snap

Page 1180 of 1474

ware		Networking CVE ID : CVE-2021-1972					
ware							
ware							
08-Sep-21	3.6	Buffer over read could occur due to incorrect check of buffer size while flashing emmc devices in Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking CVE ID : CVE-2021-1928	https://www. qualcomm.co m/company/ product- security/bull etins/august- 2021-bulletin	0-QUA-QCN9- 200921/3023			
08-Sep-21	10	Possible buffer overflow due to improper validation of device types during P2P search in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Woice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking CVE ID : CVE-2021-1972	https://www. qualcomm.co m/company/ product- security/bull etins/august- 2021-bulletin	0-QUA-QCN9- 200921/3024			
qcn9022_firmware							
08-Sep-21	3.6	Buffer over read could occur due to incorrect check of buffer size while flashing emmc devices in Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon	https://www. qualcomm.co m/company/ product- security/bull etins/august-	0-QUA-QCN9- 200921/3025			
	08-Sep-21	08-Sep-21 10 ware 08-Sep-21 3.6	D8-Sep-213.6Connectivity, Snapdragon Consumer IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and NetworkingD8-Sep-218.6Possible buffer overflow due to improper validation of device types during P2P search in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer IOT, Snapdragon Consumer IOT, Snapdragon Consumer IOT, Snapdragon Consumer IOT, Snapdragon Mobile, Snapdragon Noice & Music, Snapdragon Voice & Music, Snapdragon Wired Infrastructure and NetworkingD8-Sep-2110Snapdragon Wired Infrastructure and NetworkingD8-Sep-213.6Buffer over read could occur due to incorrect check of buffer size while flashing emmc devices in Snapdragon Connectivity, Snapdragon Connectivity, Snapdragon Connectivity, Snapdragon Connectivity, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Sonapdragon Sonapdragon Wired Infrastructure and NetworkingD8-Sep-213.6Buffer over read could occur due to incorrect check of buffer size while flashing emmc devices in Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Consumer IOT, Snapdragon	D8-Sep-213.6Connectivity, Snapdragon Consumer IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networkingmcompany/ product- security/bull etins/august- 2021-bulletinD8-Sep-217Possible buffer overflow due to improper validation of device types during P2P search in Snapdragon Consumer IOT, Snapdragon Consumer IOT, Snapdragon Consumer IOT, Snapdragon Consumer IOT, Snapdragon Mobile, Snapdragon Mobile, Snapdragon Wired Infrastructure and Networkinghttps://www. qualcomm.co m/company/ product- security/bull etins/august- 2021-bulletinD8-Sep-2110Snapdragon Industrial IOT, 			

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking	2021-bulletin	
			CVE ID : CVE-2021-1928		
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	08-Sep-21	10	Possible buffer overflow due to improper validation of device types during P2P search in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Woice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking CVE ID : CVE-2021-1972	https://www. qualcomm.co m/company/ product- security/bull etins/august- 2021-bulletin	0-QUA-QCN9- 200921/3026
qcn9024_firm	nware				
Out-of- bounds Read	08-Sep-21	3.6	Buffer over read could occur due to incorrect check of buffer size while flashing emmc devices in Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking CVE ID : CVE-2021-1928	https://www. qualcomm.co m/company/ product- security/bull etins/august- 2021-bulletin	0-QUA-QCN9- 200921/3027
Buffer Copy without	08-Sep-21	10	Possible buffer overflow due to improper validation of	https://www. qualcomm.co	0-QUA-QCN9- 200921/3028

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Checking Size of Input ('Classic Buffer Overflow')			device types during P2P search in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Woice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking CVE ID : CVE-2021-1972	m/company/ product- security/bull etins/august- 2021-bulletin	
qcn9070_firr	nware				
Out-of- bounds Read	08-Sep-21	3.6	Buffer over read could occur due to incorrect check of buffer size while flashing emmc devices in Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking CVE ID : CVE-2021-1928	https://www. qualcomm.co m/company/ product- security/bull etins/august- 2021-bulletin	0-QUA-QCN9- 200921/3029
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	08-Sep-21	10	Possible buffer overflow due to improper validation of device types during P2P search in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Woice & Music, Snapdragon Wearables, Snapdragon Wired	https://www. qualcomm.co m/company/ product- security/bull etins/august- 2021-bulletin	0-QUA-QCN9- 200921/3030

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID		
			Infrastructure and Networking				
			C				
			CVE ID : CVE-2021-1972				
qcn9072_firm	nware			1	1		
Out-of- bounds Read	08-Sep-21	3.6	Buffer over read could occur due to incorrect check of buffer size while flashing emmc devices in Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking CVE ID : CVE-2021-1928	https://www. qualcomm.co m/company/ product- security/bull etins/august- 2021-bulletin	0-QUA-QCN9- 200921/3031		
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	08-Sep-21	10	Possible buffer overflow due to improper validation of device types during P2P search in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Woice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking CVE ID : CVE-2021-1972	https://www. qualcomm.co m/company/ product- security/bull etins/august- 2021-bulletin	0-QUA-QCN9- 200921/3032		
qcn9074_firmware							
Out-of- bounds Read	08-Sep-21	3.6	Buffer over read could occur due to incorrect check of buffer size while flashing emmc devices in Snapdragon Connectivity, Snapdragon	https://www. qualcomm.co m/company/ product- security/bull	0-QUA-QCN9- 200921/3033		
CVSS Scoring Sc	ale 0-1	1-2	2-3 3-4 4-5 5-6	6-7 7-8	8-9 9-10		

Buffer Copy without Checking Size of Input (Classic Buffer Coverflow')ReadConsumer IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wearables, Snapdragon Wearables, Snapdragon Auto, Snapdragon Compute, Snapdragon Compute, Snapdragon Compute, Snapdragon Consumer IOT, Snapdragon Compute, Snapdragon Compute, Snapdragon Compute, Snapdragon Comsumer IOT, Snapdragon Consumer IOT, Snapdragon Comsumer IOT, Snapdragon Nobile, Snapdragon Nobile, Snapdragon Voice & Music, Snapdragon Voice & Music, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wearables, Snapdragon Wearables, Snapdragon Wearables, Snapdragon Wearables, Snapdragon With Infrastructure and Networking CVE ID : CVE-2021-1972https://www. qualcomm.co m/company/ product- security/bull etins/august- 2021-bulletino-QUA-QCN9- 20921/3034Out-of- bounds Read08-Sep-213.6Buffer over read could occur due to incorrect check of buffer size while flashing emmc devices in Snapdragon Mobile, S	Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')or improper validation of device types during P2P search in Snapdragon Auto, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Mustrial IOT, Snapdragon Mobile, Snapdragon Wierd Infrastructure and Networkinghttps://www. qualcomm.co m/company/ product- security/bull etins/august- 2021-bulletino-QUA-QCN9- 20921/3034Out-of- Dounds Read08-Sep-21aBuffer over read could occur due to incorrect check of buffer size while flashing emmc devices in Snapdragon Vice ID : CVE-2021-1972https://www. qualcomm.co m/company/ product- security/bull etins/august- 2021-bulletino-QUA-QCN9- 20921/3034Out-of- bounds Read08-Sep-21Buffer over read could occur due to incorrect check of buffer size while flashing emmc devices in Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Voice & Music, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Weired Infrastructure and Networkinghttps://www. qualcomm.co m/company/ product- security/bull etins/august- 2021-bulletino-QUA-QCN9- 20921/3035				Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking		
Out-of- bounds08-Sep-218.6Buffer over read could occur due to incorrect check of buffer size while flashing emmc devices in Snapdragon Connectivity, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Mobile, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networkinghttps://www. qualcomm.co m/company/ product- security/bull 	without Checking Size of Input ('Classic Buffer	08-Sep-21	10	to improper validation of device types during P2P search in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Woice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking	qualcomm.co m/company/ product- security/bull etins/august-	
Out-of- bounds Read08-Sep-213.6due to incorrect check of buffer size while flashing emmc devices in Snapdragon Connectivity, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networkinghttps://www. qualcomm.co m/company/ product- security/bull etins/august- 2021-bulletin0-QUA-QCN9- 200921/3035	qcn9100_firm	nware				
Buffer Copy 08-Sep-21 10 Possible buffer overflow due https://www. 0-QUA-QCN9-	bounds	08-Sep-21	3.6	due to incorrect check of buffer size while flashing emmc devices in Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking	qualcomm.co m/company/ product- security/bull etins/august-	• •
	Buffer Copy	08-Sep-21	10	Possible buffer overflow due	https://www.	0-QUA-QCN9-

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
without Checking Size of Input ('Classic Buffer Overflow')			to improper validation of device types during P2P search in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Woice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking CVE ID : CVE-2021-1972	qualcomm.co m/company/ product- security/bull etins/august- 2021-bulletin	200921/3036
qcs2290_firm	nware				
Exposure of Resource to Wrong Sphere	08-Sep-21	2.1	Child process can leak information from parent process due to numeric pids are getting compared and these pid can be reused in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wearables CVE ID : CVE-2021-1904	https://www. qualcomm.co m/company/ product- security/bull etins/august- 2021-bulletin	0-QUA-QCS2- 200921/3037
Incorrect Type Conversion or Cast	08-Sep-21	4.6	Incorrect pointer argument passed to trusted application TA could result in un- intended memory operations in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Industrial IOT CVE ID : CVE-2021-1923	https://www. qualcomm.co m/company/ product- security/bull etins/august- 2021-bulletin	0-QUA-QCS2- 200921/3038

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID	
Exposure of Resource to Wrong Sphere	08-Sep-21	2.1	Lack of strict validation of bootmode can lead to information disclosure in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wearables CVE ID : CVE-2021-1929	https://www. qualcomm.co m/company/ product- security/bull etins/august- 2021-bulletin	0-QUA-QCS2- 200921/3039	
Improper Restriction of Operations within the Bounds of a Memory Buffer	08-Sep-21	3.6	Possible out of bounds read due to incorrect validation of incoming buffer length in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile CVE ID : CVE-2021-1930	https://www. qualcomm.co m/company/ product- security/bull etins/august- 2021-bulletin	0-QUA-QCS2- 200921/3040	
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	08-Sep-21	10	Possible buffer overflow due to improper validation of device types during P2P search in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Industrial IOT, Snapdragon Woile, Snapdragon Woice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking CVE ID : CVE-2021-1972	https://www. qualcomm.co m/company/ product- security/bull etins/august- 2021-bulletin	0-QUA-QCS2- 200921/3041	
qcs405_firmware						
Exposure of	08-Sep-21	2.1	Child process can leak	https://www.	0-QUA-QCS4-	
CVSS Scoring Sc	ale 0-1	1-2	2-3 3-4 4-5 5-6 Page 1187 of 1474	6-7 7-8	8-9 9-10	

Wrong Spherem/company/ process due to numeric pids are getting compared and these pid can be reused in Snapdragon Auto, Snapdragon Consumer IOT, Snapdragon Mobile, Snapdragon Mobile, Snapdragon Wearables CVE ID : CVE-2021-1904m/company/ product- security/bull etins/august- 2021-bulletinBuffer Copy without Checking Size of Input (Classic Buffer08-Sep-21IPossible buffer overflow due to improper validation of device types during P2P search in Snapdragon Mobile, Snapdragon Consumer IOT, Snapdragon Consumer IOT, Snapdragon Compute, Snapdragon Compute, Snapdragon Consumer IOT, Snapdragon Mobile, Snapdragon Consumer IOT, Snapdragon Mobile, Snapdragon Wired Infrastructure and Networking CVE ID : CVE-2021-1972https://www. qualcomm.co m/company/ product- security/bull etins/august- 2021-bulletinexposure of Resource to Wrong Sphere08-Sep-21Z.1Child process can leak information from parent process due to numeric pids are getting compared and these pid can be reused in Snapdragon Connectivity, Snapdragon Connectivit	Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')Possible buffer overflow due to improper validation of device types during P2P search in Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Consumer IOT, Snapdragon Nobile, Snapdragon Nobile, Snapdragon Voice & Music, Snapdragon Wired Infrastructure and Networking CVE ID : CVE-2021-1972https://www. qualcomm.co m/company/ product- security/bull etins/august- 2021-bulletin0-QUA-QC 200921/3gesture of Resource to Wrong Sphere08-Sep-212.1Child process can leak information from parent process due to numeric pids are getting compared and these pid can be reused in Snapdragon Auto, Snapdragon Connectivity, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT,https://www. product- scurity/bull etins/august- 2021-bulletin	Wrong			process due to numeric pids are getting compared and these pid can be reused in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wearables	m/company/ product- security/bull etins/august-	200921/3042
Exposure of Resource to Wrong Sphere08-Sep-212.1Child process can leak information from parent process due to numeric pids are getting compared and these pid can be reused in Snapdragon Auto, Snapdragon Connectivity, Snapdragon Consumer IOT,https://www. qualcomm.co m/company/ product- security/bull etins/august- 2021-bulletin0-QUA-QO 200921/3	without Checking Size of Input ('Classic Buffer	08-Sep-21	10	to improper validation of device types during P2P search in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Woice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking	qualcomm.co m/company/ product- security/bull etins/august-	0-QUA-QCS4- 200921/3043
Exposure of Resource to Wrong Sphere08-Sep-212.1information from parent process due to numeric pids are getting compared and these pid can be reused in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer IOT,https://www. qualcomm.co m/company/ product- security/bull etins/august- 200921/3	qcs410_firmv	ware			L	I
Shapuragon muusu iai 101,	Resource to Wrong	08-Sep-21	2.1	information from parent process due to numeric pids are getting compared and these pid can be reused in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity,	qualcomm.co m/company/ product- security/bull etins/august-	0-QUA-QCS4- 200921/3044

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables CVE ID : CVE-2021-1904		
Loop with Unreachable Exit Condition ('Infinite Loop')	08-Sep-21	5	Loop with unreachable exit condition may occur due to improper handling of unsupported input in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Voice & Music, Snapdragon Wearables CVE ID : CVE-2021-1914	https://www. qualcomm.co m/company/ product- security/bull etins/august- 2021-bulletin	0-QUA-QCS4- 200921/3045
Out-of- bounds Write	08-Sep-21	10	Possible buffer underflow due to lack of check for negative indices values when processing user provided input in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Voice & Music, Snapdragon Wearables CVE ID : CVE-2021-1916	https://www. qualcomm.co m/company/ product- security/bull etins/august- 2021-bulletin	0-QUA-QCS4- 200921/3046
Integer Underflow (Wrap or Wraparoun d)	08-Sep-21	10	Integer underflow can occur when the RTCP length is lesser than than the actual blocks present in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT,	https://www. qualcomm.co m/company/ product- security/bull etins/august- 2021-bulletin	0-QUA-QCS4- 200921/3047

0-1 1-2

5-6

6-7

7-8

8-9

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Snapdragon IoT, Snapdragon Voice & Music, Snapdragon Wearables		
			CVE ID : CVE-2021-1919		
Integer Underflow (Wrap or Wraparoun d)	08-Sep-21	10	Integer underflow can occur due to improper handling of incoming RTCP packets in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Voice & Music, Snapdragon Wearables	https://www. qualcomm.co m/company/ product- security/bull etins/august- 2021-bulletin	0-QUA-QCS4- 200921/3048
			CVE ID : CVE-2021-1920		
Improper Restriction of Operations within the Bounds of a Memory Buffer	08-Sep-21	3.6	Possible out of bounds read due to incorrect validation of incoming buffer length in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile CVE ID : CVE-2021-1930	https://www. qualcomm.co m/company/ product- security/bull etins/august- 2021-bulletin	0-QUA-QCS4- 200921/3049
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	08-Sep-21	10	Possible buffer overflow due to improper validation of device types during P2P search in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Woice & Music, Snapdragon Wearables, Snapdragon Wired	https://www. qualcomm.co m/company/ product- security/bull etins/august- 2021-bulletin	0-QUA-QCS4- 200921/3050

0-1

1-2

5-6

6-7

7-8

8-9

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Infrastructure and Networking		
			6		
4000 (CVE ID : CVE-2021-1972		
qcs4290_firn	nware			ſ	ſ
Exposure of Resource to Wrong Sphere	08-Sep-21	2.1	Child process can leak information from parent process due to numeric pids are getting compared and these pid can be reused in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wearables	https://www. qualcomm.co m/company/ product- security/bull etins/august- 2021-bulletin	0-QUA-QCS4- 200921/3051
			CVE ID : CVE-2021-1904		
Loop with Unreachable Exit Condition ('Infinite Loop')	08-Sep-21	5	Loop with unreachable exit condition may occur due to improper handling of unsupported input in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Voice & Music, Snapdragon Wearables CVE ID : CVE-2021-1914	https://www. qualcomm.co m/company/ product- security/bull etins/august- 2021-bulletin	0-QUA-QCS4- 200921/3052
			Possible buffer underflow	https://www.	
Out-of- bounds Write	08-Sep-21	10	due to lack of check for negative indices values when processing user provided input in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity,	qualcomm.co m/company/ product- security/bull etins/august- 2021-bulletin	0-QUA-QCS4- 200921/3053

		Description & CVE ID	Patch	NCIIPC ID
		Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Voice & Music, Snapdragon Wearables		
08-Sep-21	10	Integer underflow can occur when the RTCP length is lesser than than the actual blocks present in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Voice & Music, Snapdragon Wearables	https://www. qualcomm.co m/company/ product- security/bull etins/august- 2021-bulletin	0-QUA-QCS4- 200921/3054
		CVE ID : CVE-2021-1919		
08-Sep-21	10	Integer underflow can occur due to improper handling of incoming RTCP packets in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Voice & Music, Snapdragon Wearables	https://www. qualcomm.co m/company/ product- security/bull etins/august- 2021-bulletin	0-QUA-QCS4- 200921/3055
		CVE ID : CVE-2021-1920		
08-Sep-21	4.6	Incorrect pointer argument passed to trusted application TA could result in un- intended memory operations in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Industrial IOT	https://www. qualcomm.co m/company/ product- security/bull etins/august- 2021-bulletin	0-QUA-QCS4- 200921/3056
	08-Sep-21	08-Sep-21 10	Normal StateSubstrate8Substrate8Substrate9CVE ID : CVE-2021-19169Integer underflow can occur when the RTCP length is lesser than than the actual blocks present in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Voice & Music, Snapdragon Voice & Music, Snapdragon Incoming RTCP packets in Snapdragon Consumer IOT, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Industrial IOT, Snapdragon Industrial IOT, Snapdragon Industrial IOT, Snapdragon Somertivit, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snap	Nomerican seriesSubstration Industrial IOT, Snapdragon IoT, Snapdragon Voice & Music, Snapdragon WearablesInteger underflow can occur when the RTCP length is lesser than than the actual blocks present in Snapdragon Auto, Snapdragon Compute, Snapdragon Industrial IOT, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Industrial IOT, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Conpute, Snapdragon Compute, Snapdragon IoT, Snapdragon Voice & Music, Snapdragon Nangdragon IoT, Snapdragon Voice & Music, Snapdragon None Music, Snapdragon None Music, Snapdragon None Music, Snapdragon None Music, Snapdragon Noice & Music, Snapdragon Noice

Page 1192 of 1474

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2021-1923		
Exposure of Resource to Wrong Sphere	08-Sep-21	2.1	Lack of strict validation of bootmode can lead to information disclosure in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wearables CVE ID : CVE-2021-1929	https://www. qualcomm.co m/company/ product- security/bull etins/august- 2021-bulletin	0-QUA-QCS4- 200921/3057
			Possible out of bounds read		
Improper Restriction of Operations within the Bounds of a Memory Buffer	08-Sep-21	3.6	due to incorrect validation of incoming buffer length in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile CVE ID : CVE-2021-1930	https://www. qualcomm.co m/company/ product- security/bull etins/august- 2021-bulletin	0-QUA-QCS4- 200921/3058
			Possible buffer overflow due		
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	08-Sep-21	10	<pre>Possible builler overflow due to improper validation of device types during P2P search in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Woice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking CVE ID : CVE-2021-1972</pre>	https://www. qualcomm.co m/company/ product- security/bull etins/august- 2021-bulletin	0-QUA-QCS4- 200921/3059
qcs603_firm	ware				
CVSS Scoring Sc	ale 0-1	1-2	2-3 3-4 4-5 5-6	6-7 7-8	8-9 9-10
			Page 1193 of 1474		

Exposure of Resource to Wrong Sphere08-Sep-21Z.IChild process can leak information from parent process due to numeric pids are getting compared and these pid can be reused in Snapdragon Conneutivity, Snapdragon Consumer 107, Snapdragon Mubolie, Snapdragon Nobile, Snapdragon Notice & Music, Snapdragon Notice & Music, Snapdragon Nobile, Snapdragon Notice & Music, Snapdragon Notice & Mu	Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Loop with Unreachable Exit Condition ('Infinite Loop')08-Sep-215condition may occur due to improper handling of unsupported input in Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Wearableshttps://www. qualcomm.co m/company/ product- security/bull etins/august- 2021-bulletin0-QUA-QCS6- 200921/3061Out-of- bounds Write08-Sep-2110Possible buffer underflow due to lack of check for negative indices values when processing user provided input in Snapdragon Auto, Snapdragon Connectivity, Snapdragon Connectivity, Snapdragon Connectivity, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdra	Resource to Wrong	08-Sep-21	2.1	information from parent process due to numeric pids are getting compared and these pid can be reused in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wearables	qualcomm.co m/company/ product- security/bull etins/august-	
Out-of- bounds08-Sep-2110due to lack of check for negative indices values when processing user provided input in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragonhttps://www. qualcomm.co m/company/ product- security/bull etins/august- 2021-bulletinO-QUA-QCS6- 200921/3062	Unreachable Exit Condition ('Infinite	08-Sep-21	5	condition may occur due to improper handling of unsupported input in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Voice & Music, Snapdragon Wearables	qualcomm.co m/company/ product- security/bull etins/august-	
	bounds	08-Sep-21	10	due to lack of check for negative indices values when processing user provided input in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Voice & Music, Snapdragon	qualcomm.co m/company/ product- security/bull etins/august-	e e

Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
		CVE ID : CVE-2021-1916		
08-Sep-21	10	Integer underflow can occur when the RTCP length is lesser than than the actual blocks present in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Voice & Music, Snapdragon Wearables CVE ID : CVE-2021-1919	https://www. qualcomm.co m/company/ product- security/bull etins/august- 2021-bulletin	0-QUA-QCS6- 200921/3063
08-Sep-21	10	Integer underflow can occur due to improper handling of incoming RTCP packets in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Voice & Music, Snapdragon Wearables CVE ID : CVE-2021-1920	https://www. qualcomm.co m/company/ product- security/bull etins/august- 2021-bulletin	0-QUA-QCS6- 200921/3064
08-Sep-21	2.1	Lack of strict validation of bootmode can lead to information disclosure in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wearables CVE ID : CVE-2021-1929	https://www. qualcomm.co m/company/ product- security/bull etins/august- 2021-bulletin	0-QUA-QCS6- 200921/3065
08-Sep-21	10	Possible buffer overflow due to improper validation of	https://www. qualcomm.co	0-QUA-QCS6- 200921/3066
	08-Sep-21 08-Sep-21	- -	Image: construct of the series of the seri	Image: Note of the image: Note of t

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Checking Size of Input ('Classic Buffer Overflow')			device types during P2P search in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Woice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking CVE ID : CVE-2021-1972	m/company/ product- security/bull etins/august- 2021-bulletin	
qcs605_firm	ware				
Exposure of Resource to Wrong Sphere	08-Sep-21	2.1	Child process can leak information from parent process due to numeric pids are getting compared and these pid can be reused in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables CVE ID : CVE-2021-1904	https://www. qualcomm.co m/company/ product- security/bull etins/august- 2021-bulletin	0-QUA-QCS6- 200921/3067
Loop with Unreachable Exit Condition ('Infinite Loop')	08-Sep-21	5	Loop with unreachable exit condition may occur due to improper handling of unsupported input in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Voice & Music, Snapdragon	https://www. qualcomm.co m/company/ product- security/bull etins/august- 2021-bulletin	0-QUA-QCS6- 200921/3068

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Wearables		
			CVE ID : CVE-2021-1914		
Out-of- bounds Write	08-Sep-21	10	Possible buffer underflow due to lack of check for negative indices values when processing user provided input in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Voice & Music, Snapdragon Wearables	https://www. qualcomm.co m/company/ product- security/bull etins/august- 2021-bulletin	0-QUA-QCS6- 200921/3069
			CVE ID : CVE-2021-1916		
Integer Underflow (Wrap or Wraparoun d)	08-Sep-21	10	Integer underflow can occur when the RTCP length is lesser than than the actual blocks present in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Voice & Music, Snapdragon Wearables CVE ID : CVE-2021-1919	https://www. qualcomm.co m/company/ product- security/bull etins/august- 2021-bulletin	0-QUA-QCS6- 200921/3070
Integer Underflow (Wrap or Wraparoun d)	08-Sep-21	10	Integer underflow can occur due to improper handling of incoming RTCP packets in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Voice & Music, Snapdragon Wearables	https://www. qualcomm.co m/company/ product- security/bull etins/august- 2021-bulletin	0-QUA-QCS6- 200921/3071
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-2021-1920		
Exposure of Resource to Wrong Sphere	08-Sep-21	2.1	Lack of strict validation of bootmode can lead to information disclosure in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wearables CVE ID : CVE-2021-1929	https://www. qualcomm.co m/company/ product- security/bull etins/august- 2021-bulletin	0-QUA-QCS6- 200921/3072
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	08-Sep-21	10	Possible buffer overflow due to improper validation of device types during P2P search in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Woice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking CVE ID : CVE-2021-1972	https://www. qualcomm.co m/company/ product- security/bull etins/august- 2021-bulletin	0-QUA-QCS6- 200921/3073
qcs610_firm	ware				
Exposure of Resource to Wrong Sphere	08-Sep-21	2.1	Child process can leak information from parent process due to numeric pids are getting compared and these pid can be reused in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT,	https://www. qualcomm.co m/company/ product- security/bull etins/august- 2021-bulletin	0-QUA-QCS6- 200921/3074

CVSS Scoring Scale	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10
			Pa	ge 1198	of 1474					

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables CVE ID : CVE-2021-1904		
Loop with Unreachable Exit Condition ('Infinite Loop')	08-Sep-21	5	Loop with unreachable exit condition may occur due to improper handling of unsupported input in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Voice & Music, Snapdragon Wearables CVE ID : CVE-2021-1914	https://www. qualcomm.co m/company/ product- security/bull etins/august- 2021-bulletin	0-QUA-QCS6- 200921/3075
Out-of- bounds Write	08-Sep-21	10	Possible buffer underflow due to lack of check for negative indices values when processing user provided input in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Voice & Music, Snapdragon Wearables CVE ID : CVE-2021-1916	https://www. qualcomm.co m/company/ product- security/bull etins/august- 2021-bulletin	0-QUA-QCS6- 200921/3076
Integer Underflow (Wrap or Wraparoun d)	08-Sep-21	10	Integer underflow can occur when the RTCP length is lesser than than the actual blocks present in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT,	https://www. qualcomm.co m/company/ product- security/bull etins/august- 2021-bulletin	0-QUA-QCS6- 200921/3077

0-1 1-2

5-6

6-7

7-8

8-9

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Snapdragon IoT, Snapdragon Voice & Music, Snapdragon Wearables		
			CVE ID : CVE-2021-1919		
Integer Underflow (Wrap or Wraparoun d)	08-Sep-21	10	Integer underflow can occur due to improper handling of incoming RTCP packets in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Voice & Music, Snapdragon Wearables CVE ID : CVE-2021-1920	https://www. qualcomm.co m/company/ product- security/bull etins/august- 2021-bulletin	0-QUA-QCS6- 200921/3078
Exposure of Resource to Wrong Sphere	08-Sep-21	2.1	Lack of strict validation of bootmode can lead to information disclosure in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wearables CVE ID : CVE-2021-1929	https://www. qualcomm.co m/company/ product- security/bull etins/august- 2021-bulletin	0-QUA-QCS6- 200921/3079
Improper Restriction of Operations within the Bounds of a Memory Buffer	08-Sep-21	3.6	Possible out of bounds read due to incorrect validation of incoming buffer length in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile CVE ID : CVE-2021-1930	https://www. qualcomm.co m/company/ product- security/bull etins/august- 2021-bulletin	0-QUA-QCS6- 200921/3080

CVSS Scoring Scale	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10
Page 1200 of 1474										

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	08-Sep-21	10	Possible buffer overflow due to improper validation of device types during P2P search in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Woice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking CVE ID : CVE-2021-1972	https://www. qualcomm.co m/company/ product- security/bull etins/august- 2021-bulletin	0-QUA-QCS6- 200921/3081
qcs6125_firm	nware			·	·
Exposure of Resource to Wrong Sphere	08-Sep-21	2.1	Child process can leak information from parent process due to numeric pids are getting compared and these pid can be reused in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wearables CVE ID : CVE-2021-1904	https://www. qualcomm.co m/company/ product- security/bull etins/august- 2021-bulletin	0-QUA-QCS6- 200921/3082
Loop with Unreachable Exit Condition ('Infinite Loop')	08-Sep-21	5	Loop with unreachable exit condition may occur due to improper handling of unsupported input in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT,	https://www. qualcomm.co m/company/ product- security/bull etins/august- 2021-bulletin	0-QUA-QCS6- 200921/3083

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Snapdragon IoT, Snapdragon Voice & Music, Snapdragon Wearables		
			CVE ID : CVE-2021-1914		
Out-of- bounds Write	08-Sep-21	10	Possible buffer underflow due to lack of check for negative indices values when processing user provided input in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Voice & Music, Snapdragon Wearables	https://www. qualcomm.co m/company/ product- security/bull etins/august- 2021-bulletin	0-QUA-QCS6- 200921/3084
			CVE ID : CVE-2021-1916		
Integer Underflow (Wrap or Wraparoun d)	08-Sep-21	10	Integer underflow can occur when the RTCP length is lesser than than the actual blocks present in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Voice & Music, Snapdragon Wearables	https://www. qualcomm.co m/company/ product- security/bull etins/august- 2021-bulletin	0-QUA-QCS6- 200921/3085
			CVE ID : CVE-2021-1919		
Integer Underflow (Wrap or Wraparoun d)	08-Sep-21	10	Integer underflow can occur due to improper handling of incoming RTCP packets in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon	https://www. qualcomm.co m/company/ product- security/bull etins/august- 2021-bulletin	0-QUA-QCS6- 200921/3086

0-1

1-2

2-3 3-4

4-5

5-6

6-7

7-8

8-9

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Voice & Music, Snapdragon Wearables CVE ID : CVE-2021-1920		
Exposure of Resource to Wrong Sphere	08-Sep-21	2.1	Lack of strict validation of bootmode can lead to information disclosure in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wearables CVE ID : CVE-2021-1929	https://www. qualcomm.co m/company/ product- security/bull etins/august- 2021-bulletin	0-QUA-QCS6- 200921/3087
Improper Restriction of Operations within the Bounds of a Memory Buffer	08-Sep-21	3.6	Possible out of bounds read due to incorrect validation of incoming buffer length in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile CVE ID : CVE-2021-1930	https://www. qualcomm.co m/company/ product- security/bull etins/august- 2021-bulletin	0-QUA-QCS6- 200921/3088
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	08-Sep-21	10	Possible buffer overflow due to improper validation of device types during P2P search in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Industrial IOT, Snapdragon Woile, Snapdragon Woice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking	https://www. qualcomm.co m/company/ product- security/bull etins/august- 2021-bulletin	0-QUA-QCS6- 200921/3089
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 & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2021-1972		
qcx315_firm	ware				
Exposure of Resource to Wrong Sphere	08-Sep-21	2.1	Child process can leak information from parent process due to numeric pids are getting compared and these pid can be reused in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables CVE ID : CVE-2021-1904	https://www. qualcomm.co m/company/ product- security/bull etins/august- 2021-bulletin	0-QUA-QCX3- 200921/3090
Loop with Unreachable Exit Condition ('Infinite Loop')	08-Sep-21	5	Loop with unreachable exit condition may occur due to improper handling of unsupported input in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Voice & Music, Snapdragon Wearables CVE ID : CVE-2021-1914	https://www. qualcomm.co m/company/ product- security/bull etins/august- 2021-bulletin	0-QUA-QCX3- 200921/3091
Out-of- bounds Write	08-Sep-21	10	Possible buffer underflow due to lack of check for negative indices values when processing user provided input in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT,	https://www. qualcomm.co m/company/ product- security/bull etins/august- 2021-bulletin	0-QUA-QCX3- 200921/3092

0-1

1-2

5-6

6-7

7-8

8-9

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Snapdragon IoT, Snapdragon Voice & Music, Snapdragon Wearables		
			CVE ID : CVE-2021-1916		
Integer Underflow (Wrap or Wraparoun d)	08-Sep-21	10	Integer underflow can occur when the RTCP length is lesser than than the actual blocks present in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Voice & Music, Snapdragon Wearables	https://www. qualcomm.co m/company/ product- security/bull etins/august- 2021-bulletin	0-QUA-QCX3- 200921/3093
			CVE ID : CVE-2021-1919		
Integer Underflow (Wrap or Wraparoun d)	08-Sep-21	10	Integer underflow can occur due to improper handling of incoming RTCP packets in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Voice & Music, Snapdragon Wearables	https://www. qualcomm.co m/company/ product- security/bull etins/august- 2021-bulletin	0-QUA-QCX3- 200921/3094
			CVE ID : CVE-2021-1920		
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	08-Sep-21	10	Possible buffer overflow due to improper validation of device types during P2P search in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music,	https://www. qualcomm.co m/company/ product- security/bull etins/august- 2021-bulletin	0-QUA-QCX3- 200921/3095

0-1

1-2

2-3 3-4 4-5 Page 1205 of 1474 7-8

5-6

6-7

8-9

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking		
			CVE ID : CVE-2021-1972		
qet4101_firm	nware			l	
Exposure of Resource to Wrong Sphere	08-Sep-21	2.1	Child process can leak information from parent process due to numeric pids are getting compared and these pid can be reused in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wearables CVE ID : CVE-2021-1904	https://www. qualcomm.co m/company/ product- security/bull etins/august- 2021-bulletin	O-QUA-QET4- 200921/3096
qfe1922_firm	nware				
Out-of- bounds Read	08-Sep-21	3.6	Buffer over read could occur due to incorrect check of buffer size while flashing emmc devices in Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking CVE ID : CVE-2021-1928	https://www. qualcomm.co m/company/ product- security/bull etins/august- 2021-bulletin	O-QUA-QFE1- 200921/3097
Buffer Copy without Checking Size of Input	08-Sep-21	10	Possible buffer overflow due to improper validation of device types during P2P search in Snapdragon Auto,	https://www. qualcomm.co m/company/ product-	0-QUA-QFE1- 200921/3098
CVSS Scoring Sc	ale 0-1	1-2	2-3 3-4 4-5 5-6	6-7 7-8	8-9 9-10

Page 1206 of 1474

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
('Classic Buffer Overflow')			Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking CVE ID : CVE-2021-1972	security/bull etins/august- 2021-bulletin	
qfe1952_firn	nware				
Out-of- bounds Read	08-Sep-21	3.6	Buffer over read could occur due to incorrect check of buffer size while flashing emmc devices in Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking CVE ID : CVE-2021-1928	https://www. qualcomm.co m/company/ product- security/bull etins/august- 2021-bulletin	O-QUA-QFE1- 200921/3099
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	08-Sep-21	10	Possible buffer overflow due to improper validation of device types during P2P search in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Woice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and	https://www. qualcomm.co m/company/ product- security/bull etins/august- 2021-bulletin	O-QUA-QFE1- 200921/3100

CVSS Scoring Scale	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10
	Page 1207 of 1474									

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID			
			Networking					
			CVE ID : CVE-2021-1972					
qrb5165_firm	qrb5165_firmware							
Exposure of Resource to Wrong Sphere	08-Sep-21	2.1	Child process can leak information from parent process due to numeric pids are getting compared and these pid can be reused in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wearables CVE ID : CVE-2021-1904	https://www. qualcomm.co m/company/ product- security/bull etins/august- 2021-bulletin	O-QUA-QRB5- 200921/3101			
Improper Restriction of Operations within the Bounds of a Memory Buffer	08-Sep-21	3.6	Possible out of bounds read due to incorrect validation of incoming buffer length in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile CVE ID : CVE-2021-1930	https://www. qualcomm.co m/company/ product- security/bull etins/august- 2021-bulletin	0-QUA-QRB5- 200921/3102			
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	08-Sep-21	10	Possible buffer overflow due to improper validation of device types during P2P search in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables,	https://www. qualcomm.co m/company/ product- security/bull etins/august- 2021-bulletin	0-QUA-QRB5- 200921/3103			
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 & CVE ID	Patch	NCIIPC ID			
			Snapdragon Wired Infrastructure and Networking					
			CVE ID : CVE-2021-1972					
qsm8250_fir	qsm8250_firmware							
Exposure of Resource to Wrong Sphere	08-Sep-21	2.1	Child process can leak information from parent process due to numeric pids are getting compared and these pid can be reused in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wearables CVE ID : CVE-2021-1904	https://www. qualcomm.co m/company/ product- security/bull etins/august- 2021-bulletin	O-QUA-QSM8- 200921/3104			
Improper Restriction of Operations within the Bounds of a Memory Buffer	08-Sep-21	3.6	Possible out of bounds read due to incorrect validation of incoming buffer length in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile CVE ID : CVE-2021-1930	https://www. qualcomm.co m/company/ product- security/bull etins/august- 2021-bulletin	0-QUA-QSM8- 200921/3105			
qsm8350_fir	mware	_						
Incorrect Type Conversion or Cast	08-Sep-21	4.6	Incorrect pointer argument passed to trusted application TA could result in un- intended memory operations in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity,	https://www. qualcomm.co m/company/ product- security/bull etins/august- 2021-bulletin	O-QUA-QSM8- 200921/3106			

CVSS Scoring Scale	0-1	1-2	2-3

4-5

5-6

6-7

7-8

8-9

9-10

		Snapdragon Industrial IOT		
		CVE ID : CVE-2021-1923		
08-Sep-21	3.6	Possible out of bounds read due to incorrect validation of incoming buffer length in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile CVE ID : CVE-2021-1930	https://www. qualcomm.co m/company/ product- security/bull etins/august- 2021-bulletin	0-QUA-QSM8- 200921/3107
nware				
08-Sep-21	2.1	Child process can leak information from parent process due to numeric pids are getting compared and these pid can be reused in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wearables CVE ID : CVE-2021-1904	https://www. qualcomm.co m/company/ product- security/bull etins/august- 2021-bulletin	0-QUA-QSW8- 200921/3108
08-Sep-21	5	Loop with unreachable exit condition may occur due to improper handling of unsupported input in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Voice & Music, Snapdragon	https://www. qualcomm.co m/company/ product- security/bull etins/august- 2021-bulletin	0-QUA-QSW8- 200921/3109
	nware 08-Sep-21	nware 08-Sep-21 2.1 08-Sep-21 5	08-Sep-21a.6due to incorrect validation of incoming buffer length in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer IOT, Snapdragon Mobile CVE ID : CVE-2021-1930CVE ID : CVE-2021-1930 Child process can leak information from parent process due to numeric pids are getting compared and these pid can be reused in Snapdragon Consumer IOT, Snapdragon Auto,08-Sep-212.12.1Snapdragon Compute, Snapdragon Compute, Snapdragon Consumer IOT, Snapdragon Compute, Snapdragon Consumer IOT, Snapdragon Consumer IOT, Snapdragon Consumer IOT, Snapdragon Consumer IOT, Snapdragon Mobile, Snapdragon Nobile, Snapdragon Nobile, Snapdragon Nobile, Snapdragon Nobile, Snapdragon Nobile, Snapdragon Nobile, Snapdragon Mobile, Snapdragon Mobile, Snapdragon Mobile, Snapdragon Mobile, Snapdragon Mobile, Snapdragon Mobile, Snapdragon Nobile, Snapdragon Mobile, Snapdragon Nobile, Snapdragon Nobile, Snapdragon Nobile, Snapdragon Mobile, Snapdragon Mobile, Snapdragon Mobile, Snapdragon Mobile, Snapdragon Mobile, Snapdragon Nobile, Snapdragon Nobile, <	08-Sep-213.6due to incorrect validation of incoming buffer length in Snapdragon Compute, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile CVE ID : CVE-2021-1930https://www. qualcomm.co m/company/ product- security/bull etins/august- 2021-bulletinnware

Page 1210 of 1474

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Wearables		
			CVE ID : CVE-2021-1914		
Out-of- bounds Write	08-Sep-21	10	Possible buffer underflow due to lack of check for negative indices values when processing user provided input in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Voice & Music, Snapdragon Wearables	https://www. qualcomm.co m/company/ product- security/bull etins/august- 2021-bulletin	0-QUA-QSW8- 200921/3110
			CVE ID : CVE-2021-1916		
Integer Underflow (Wrap or Wraparoun d)	08-Sep-21	10	Integer underflow can occur when the RTCP length is lesser than than the actual blocks present in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Voice & Music, Snapdragon Wearables CVE ID : CVE-2021-1919	https://www. qualcomm.co m/company/ product- security/bull etins/august- 2021-bulletin	0-QUA-QSW8- 200921/3111
Integer Underflow (Wrap or Wraparoun d)	08-Sep-21	10	Integer underflow can occur due to improper handling of incoming RTCP packets in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Voice & Music, Snapdragon Wearables	https://www. qualcomm.co m/company/ product- security/bull etins/august- 2021-bulletin	0-QUA-QSW8- 200921/3112
CVSS Scoring Sca	ale 0-1	1-2	2-3 3-4 4-5 5-6 Page 1211 of 1474	6-7 7-8	8-9 9-10

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2021-1920		
qualcomm21	5_firmware				
Exposure of Resource to Wrong Sphere	08-Sep-21	2.1	Child process can leak information from parent process due to numeric pids are getting compared and these pid can be reused in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables CVE ID : CVE-2021-1904	https://www. qualcomm.co m/company/ product- security/bull etins/august- 2021-bulletin	0-QUA-QUAL- 200921/3113
Loop with Unreachable Exit Condition ('Infinite Loop')	08-Sep-21	5	Loop with unreachable exit condition may occur due to improper handling of unsupported input in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Voice & Music, Snapdragon Wearables CVE ID : CVE-2021-1914	https://www. qualcomm.co m/company/ product- security/bull etins/august- 2021-bulletin	0-QUA-QUAL- 200921/3114
Out-of- bounds Write	08-Sep-21	10	Possible buffer underflow due to lack of check for negative indices values when processing user provided input in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT,	https://www. qualcomm.co m/company/ product- security/bull etins/august- 2021-bulletin	0-QUA-QUAL- 200921/3115

0-1

1-2

5-6

6-7

7-8

8-9

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Snapdragon IoT, Snapdragon Voice & Music, Snapdragon Wearables		
			CVE ID : CVE-2021-1916		
Integer Underflow (Wrap or Wraparoun d)	08-Sep-21	10	Integer underflow can occur when the RTCP length is lesser than than the actual blocks present in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Voice & Music, Snapdragon Wearables CVE ID : CVE-2021-1919	https://www. qualcomm.co m/company/ product- security/bull etins/august- 2021-bulletin	O-QUA-QUAL- 200921/3116
Integer Underflow (Wrap or Wraparoun d)	08-Sep-21	10	Integer underflow can occur due to improper handling of incoming RTCP packets in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Voice & Music, Snapdragon Wearables	https://www. qualcomm.co m/company/ product- security/bull etins/august- 2021-bulletin	0-QUA-QUAL- 200921/3117
			CVE ID : CVE-2021-1920		
Out-of- bounds Read	08-Sep-21	3.6	Buffer over read could occur due to incorrect check of buffer size while flashing emmc devices in Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon	https://www. qualcomm.co m/company/ product- security/bull etins/august- 2021-bulletin	0-QUA-QUAL- 200921/3118

CVSS Scoring Scale	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-1
			Pa	age 1213	of 1474					

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Wired Infrastructure and Networking CVE ID : CVE-2021-1928		
Exposure of Resource to Wrong Sphere	08-Sep-21	2.1	Lack of strict validation of bootmode can lead to information disclosure in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wearables CVE ID : CVE-2021-1929	https://www. qualcomm.co m/company/ product- security/bull etins/august- 2021-bulletin	0-QUA-QUAL- 200921/3119
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	08-Sep-21	10	Possible buffer overflow due to improper validation of device types during P2P search in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Woice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking CVE ID : CVE-2021-1972	https://www. qualcomm.co m/company/ product- security/bull etins/august- 2021-bulletin	O-QUA-QUAL- 200921/3120
sa415m_firm	ware				
Exposure of Resource to Wrong Sphere	08-Sep-21	2.1	Child process can leak information from parent process due to numeric pids are getting compared and these pid can be reused in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity,	https://www. qualcomm.co m/company/ product- security/bull etins/august- 2021-bulletin	0-QUA-SA41- 200921/3121
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 & CVE ID	Patch	NCIIPC ID
			Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables CVE ID : CVE-2021-1904		
Loop with Unreachable Exit Condition ('Infinite Loop')	08-Sep-21	5	Loop with unreachable exit condition may occur due to improper handling of unsupported input in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Voice & Music, Snapdragon Wearables CVE ID : CVE-2021-1914	https://www. qualcomm.co m/company/ product- security/bull etins/august- 2021-bulletin	0-QUA-SA41- 200921/3122
Out-of- bounds Write	08-Sep-21	10	Possible buffer underflow due to lack of check for negative indices values when processing user provided input in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Voice & Music, Snapdragon Wearables CVE ID : CVE-2021-1916	https://www. qualcomm.co m/company/ product- security/bull etins/august- 2021-bulletin	0-QUA-SA41- 200921/3123
Integer Underflow (Wrap or Wraparoun d)	08-Sep-21	10	Integer underflow can occur when the RTCP length is lesser than than the actual blocks present in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity,	https://www. qualcomm.co m/company/ product- security/bull etins/august-	0-QUA-SA41- 200921/3124

1-2 2-3

0-1

5-6

6-7

7-8

8-9

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Voice & Music, Snapdragon Wearables CVE ID : CVE-2021-1919	2021-bulletin	
Integer Underflow (Wrap or Wraparoun d)	08-Sep-21	10	Integer underflow can occur due to improper handling of incoming RTCP packets in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Voice & Music, Snapdragon Wearables CVE ID : CVE-2021-1920	https://www. qualcomm.co m/company/ product- security/bull etins/august- 2021-bulletin	0-QUA-SA41- 200921/3125
Improper Restriction of Operations within the Bounds of a Memory Buffer	08-Sep-21	3.6	Possible out of bounds read due to incorrect validation of incoming buffer length in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile CVE ID : CVE-2021-1930	https://www. qualcomm.co m/company/ product- security/bull etins/august- 2021-bulletin	0-QUA-SA41- 200921/3126
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	08-Sep-21	10	Possible buffer overflow due to improper validation of device types during P2P search in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music,	https://www. qualcomm.co m/company/ product- security/bull etins/august- 2021-bulletin	0-QUA-SA41- 200921/3127

0-1 1-2

5-6

6-7

7-8

8-9

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking		
			CVE ID : CVE-2021-1972		
sa515m_firm	ware				
Loop with Unreachable Exit Condition ('Infinite Loop')	08-Sep-21	5	Loop with unreachable exit condition may occur due to improper handling of unsupported input in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Voice & Music, Snapdragon Wearables CVE ID : CVE-2021-1914	https://www. qualcomm.co m/company/ product- security/bull etins/august- 2021-bulletin	0-QUA-SA51- 200921/3128
Out-of- bounds Write	08-Sep-21	10	Possible buffer underflow due to lack of check for negative indices values when processing user provided input in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Voice & Music, Snapdragon Wearables CVE ID : CVE-2021-1916	https://www. qualcomm.co m/company/ product- security/bull etins/august- 2021-bulletin	0-QUA-SA51- 200921/3129
Integer Underflow (Wrap or Wraparoun d)	08-Sep-21	10	Integer underflow can occur when the RTCP length is lesser than than the actual blocks present in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity,	https://www. qualcomm.co m/company/ product- security/bull etins/august-	0-QUA-SA51- 200921/3130

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Voice & Music, Snapdragon Wearables CVE ID : CVE-2021-1919	2021-bulletin	
Integer Underflow (Wrap or Wraparoun d)	08-Sep-21	10	Integer underflow can occur due to improper handling of incoming RTCP packets in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Voice & Music, Snapdragon Wearables	https://www. qualcomm.co m/company/ product- security/bull etins/august- 2021-bulletin	0-QUA-SA51- 200921/3131
			CVE ID : CVE-2021-1920		
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	08-Sep-21	10	Possible buffer overflow due to improper validation of device types during P2P search in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Woice & Music, Snapdragon Wired Infrastructure and Networking CVE ID : CVE-2021-1972	https://www. qualcomm.co m/company/ product- security/bull etins/august- 2021-bulletin	0-QUA-SA51- 200921/3132
sa6145p_firm	nware				
Exposure of Resource to Wrong Sphere	08-Sep-21	2.1	Child process can leak information from parent process due to numeric pids are getting compared and	https://www. qualcomm.co m/company/ product-	0-QUA-SA61- 200921/3133
CVSS Scoring Sc	ale 0-1	1-2	2-3 3-4 4-5 5-6 Page 1218 of 1474	6-7 7-8	8-9 9-10

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			these pid can be reused in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables CVE ID : CVE-2021-1904	security/bull etins/august- 2021-bulletin	
Out-of- bounds Write	08-Sep-21	10	Possible buffer underflow due to lack of check for negative indices values when processing user provided input in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Voice & Music, Snapdragon Wearables CVE ID : CVE-2021-1916	https://www. qualcomm.co m/company/ product- security/bull etins/august- 2021-bulletin	0-QUA-SA61- 200921/3134
Incorrect Type Conversion or Cast	08-Sep-21	4.6	Incorrect pointer argument passed to trusted application TA could result in un- intended memory operations in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Industrial IOT CVE ID : CVE-2021-1923	https://www. qualcomm.co m/company/ product- security/bull etins/august- 2021-bulletin	0-QUA-SA61- 200921/3135
Exposure of Resource to Wrong Sphere	08-Sep-21	2.1	Lack of strict validation of bootmode can lead to information disclosure in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity,	https://www. qualcomm.co m/company/ product- security/bull etins/august-	0-QUA-SA61- 200921/3136

1-2 2-3

0-1

5-6

6-7

7-8

8-9

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wearables	2021-bulletin	
			CVE ID : CVE-2021-1929		
Improper Restriction of Operations within the Bounds of a Memory Buffer	08-Sep-21	3.6	Possible out of bounds read due to incorrect validation of incoming buffer length in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile	https://www. qualcomm.co m/company/ product- security/bull etins/august- 2021-bulletin	0-QUA-SA61- 200921/3137
			CVE ID : CVE-2021-1930		
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	08-Sep-21	10	Possible buffer overflow due to improper validation of device types during P2P search in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Woice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking CVE ID : CVE-2021-1972	https://www. qualcomm.co m/company/ product- security/bull etins/august- 2021-bulletin	0-QUA-SA61- 200921/3138
sa6150p_firm	nware				
Exposure of Resource to Wrong Sphere	08-Sep-21	2.1	Child process can leak information from parent process due to numeric pids are getting compared and these pid can be reused in Snapdragon Auto, Snapdragon Compute,	https://www. qualcomm.co m/company/ product- security/bull etins/august- 2021-bulletin	0-QUA-SA61- 200921/3139
CVSS Scoring Sc	ale 0-1	1-2	2-3 3-4 4-5 5-6 Page 1220 of 1474	6-7 7-8	8-9 9-10

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables CVE ID : CVE-2021-1904		
Out-of- bounds Write	08-Sep-21	10	Possible buffer underflow due to lack of check for negative indices values when processing user provided input in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Voice & Music, Snapdragon Wearables CVE ID : CVE-2021-1916	https://www. qualcomm.co m/company/ product- security/bull etins/august- 2021-bulletin	0-QUA-SA61- 200921/3140
Incorrect Type Conversion or Cast	08-Sep-21	4.6	Incorrect pointer argument passed to trusted application TA could result in un- intended memory operations in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Industrial IOT CVE ID : CVE-2021-1923	https://www. qualcomm.co m/company/ product- security/bull etins/august- 2021-bulletin	0-QUA-SA61- 200921/3141
Exposure of Resource to Wrong Sphere	08-Sep-21	2.1	Lack of strict validation of bootmode can lead to information disclosure in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile,	https://www. qualcomm.co m/company/ product- security/bull etins/august- 2021-bulletin	0-QUA-SA61- 200921/3142

0-1

1-2

2-3 3-4

4-5

5-6

6-7

7-8

8-9

Within the Bounds of a Memory Buffer Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')			Snapdragon Wearables						
Restriction of Operations within the Bounds of a Memory Buffer Buffer Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')				gon Wearables					
Restriction of Operations within the Bounds of a Memory Buffer Buffer Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')			CVE ID : CVE-2021-1929						
without Checking Size of Input 08-S ('Classic Buffer Overflow')	18-Sep-21	3.6	Possible out of bounds read due to incorrect validation of incoming buffer length in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile CVE ID : CVE-2021-1930	https://www. qualcomm.co m/company/ product- security/bull etins/august- 2021-bulletin	0-QUA-SA61- 200921/3143				
sa6155p_firmwar	18-Sep-21	10	Possible buffer overflow due to improper validation of device types during P2P search in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Woice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking CVE ID : CVE-2021-1972	https://www. qualcomm.co m/company/ product- security/bull etins/august- 2021-bulletin	0-QUA-SA61- 200921/3144				
	sa6155p_firmware								
Exposure of Resource to Wrong Sphere	98-Sep-21	p-21 Child process can leak information from parent process due to numeric pids are getting compared and these pid can be reused in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer IOT, Snapdragon Industrial IOT,		https://www. qualcomm.co m/company/ product- security/bull etins/august- 2021-bulletin	0-QUA-SA61- 200921/3145				

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables CVE ID : CVE-2021-1904		
Out-of- bounds Write	08-Sep-21	10	Possible buffer underflow due to lack of check for negative indices values when processing user provided input in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Voice & Music, Snapdragon Wearableshttps://www. qualcomm.co m/company/ product- security/bull etins/august- 		0-QUA-SA61- 200921/3146
Incorrect Type Conversion or Cast	08-Sep-21	4.6	CVE ID : CVE-2021-1916 Incorrect pointer argument passed to trusted application TA could result in un- intended memory operations in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Industrial IOT CVE ID : CVE-2021-1923	https://www. qualcomm.co m/company/ product- security/bull etins/august- 2021-bulletin	0-QUA-SA61- 200921/3147
Exposure of Resource to Wrong Sphere	08-Sep-21	2.1	Lack of strict validation of bootmode can lead to information disclosure in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wearables CVE ID : CVE-2021-1929	https://www. qualcomm.co m/company/ product- security/bull etins/august- 2021-bulletin	0-QUA-SA61- 200921/3148

-												
	CVSS Scoring Scale	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9		
-	Page 1223 of 1474											

9-10

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Improper Restriction of Operations within the Bounds of a Memory Buffer	08-Sep-21	3.6	Possible out of bounds read due to incorrect validation of incoming buffer length in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile CVE ID : CVE-2021-1930	https://www. qualcomm.co m/company/ product- security/bull etins/august- 2021-bulletin	0-QUA-SA61- 200921/3149
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	08-Sep-21	10	Possible buffer overflow due to improper validation of device types during P2P search in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Woice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking CVE ID : CVE-2021-1972	https://www. qualcomm.co m/company/ product- security/bull etins/august- 2021-bulletin	O-QUA-SA61- 200921/3150
sa6155_firm	ware				
Exposure of Resource to Wrong Sphere	08-Sep-21	2.1	Child process can leak information from parent process due to numeric pids are getting compared and these pid can be reused in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music,	https://www. qualcomm.co m/company/ product- security/bull etins/august- 2021-bulletin	0-QUA-SA61- 200921/3151

CVSS Scoring Scale	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10
Page 1224 of 1474										

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Snapdragon Wearables		
			CVE ID : CVE-2021-1904		
Out-of- bounds Write	08-Sep-21	10	Possible buffer underflow due to lack of check for negative indices values when processing user provided input in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Voice & Music, Snapdragon Wearables	https://www. qualcomm.co m/company/ product- security/bull etins/august- 2021-bulletin	0-QUA-SA61- 200921/3152
			CVE ID : CVE-2021-1916		
Incorrect Type Conversion or Cast	08-Sep-21	4.6	Incorrect pointer argument passed to trusted application TA could result in un- intended memory operations in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Industrial IOT CVE ID : CVE-2021-1923	https://www. qualcomm.co m/company/ product- security/bull etins/august- 2021-bulletin	0-QUA-SA61- 200921/3153
Improper Restriction of Operations within the Bounds of a Memory Buffer	08-Sep-21	Possible out of bounds read due to incorrect validation of incoming buffer length in Snapdragon Auto, Snapdragon Compute,		https://www. qualcomm.co m/company/ product- security/bull etins/august- 2021-bulletin	0-QUA-SA61- 200921/3154
Buffer Copy without Checking Size of Input	08-Sep-21	10	Possible buffer overflow due to improper validation of device types during P2P search in Snapdragon Auto,	https://www. qualcomm.co m/company/ product-	0-QUA-SA61- 200921/3155
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 & CVE ID	Patch	NCIIPC ID
('Classic Buffer Overflow')			Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking CVE ID : CVE-2021-1972	security/bull etins/august- 2021-bulletin	
sa8145p_firm	nware				
Exposure of Resource to Wrong Sphere	08-Sep-21	2.1	Child process can leak information from parent process due to numeric pids are getting compared and these pid can be reused in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wearables CVE ID : CVE-2021-1904	https://www. qualcomm.co m/company/ product- security/bull etins/august- 2021-bulletin	O-QUA-SA81- 200921/3156
Out-of- bounds Write	08-Sep-21	Possible buffer underflow due to lack of check for negative indices values wh processing user provided input in Snapdragon Auto, Snandragon Compute		https://www. qualcomm.co m/company/ product- security/bull etins/august- 2021-bulletin	0-QUA-SA81- 200921/3157

CVSS Scoring Scale	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8
			Da	οσ <u>ο</u> 1226	of 1/17/			

8-9 9-10

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2021-1916		
Incorrect Type Conversion or Cast	sion 08-Sep-21		 Incorrect pointer argument passed to trusted application TA could result in un- intended memory operations in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Industrial IOT CVE ID : CVE-2021-1923 		0-QUA-SA81- 200921/3158
Exposure of Resource to Wrong Sphere	08-Sep-21	2.1	Lack of strict validation of bootmode can lead to information disclosure in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wearables CVE ID : CVE-2021-1929	https://www. qualcomm.co m/company/ product- security/bull etins/august- 2021-bulletin	0-QUA-SA81- 200921/3159
Improper Restriction of Operations within the Bounds of a Memory Buffer	08-Sep-21	3.6	Possible out of bounds read due to incorrect validation of incoming buffer length in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile CVE ID : CVE-2021-1930	https://www. qualcomm.co m/company/ product- security/bull etins/august- 2021-bulletin	0-QUA-SA81- 200921/3160
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	08-Sep-21	10	Possible buffer overflow due to improper validation of device types during P2P search in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT,	https://www. qualcomm.co m/company/ product- security/bull etins/august- 2021-bulletin	0-QUA-SA81- 200921/3161

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking		
sa8150p_firm	nware		CVE ID : CVE-2021-1972		
Exposure of Resource to Wrong Sphere	08-Sep-21	2.1	Child process can leak information from parent process due to numeric pids are getting compared and these pid can be reused in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wearables CVE ID : CVE-2021-1904	https://www. qualcomm.co m/company/ product- security/bull etins/august- 2021-bulletin	0-QUA-SA81- 200921/3162
Out-of- bounds Write	08-Sep-21	10	Possible buffer underflow due to lack of check for negative indices values when processing user provided input in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Voice & Music, Snapdragon Wearables CVE ID : CVE-2021-1916	https://www. qualcomm.co m/company/ product- security/bull etins/august- 2021-bulletin	0-QUA-SA81- 200921/3163
Incorrect Type	08-Sep-21	4.6	Incorrect pointer argument passed to trusted application	https://www. qualcomm.co	0-QUA-SA81- 200921/3164

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Conversion or Cast			TA could result in un- intended memory operations in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Industrial IOT CVE ID : CVE-2021-1923	m/company/ product- security/bull etins/august- 2021-bulletin	
Exposure of Resource to Wrong Sphere	08-Sep-21	2.1	Lack of strict validation of bootmode can lead to information disclosure in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wearables CVE ID : CVE-2021-1929	https://www. qualcomm.co m/company/ product- security/bull etins/august- 2021-bulletin	O-QUA-SA81- 200921/3165
Improper Restriction of Operations within the Bounds of a Memory Buffer	08-Sep-21	3.6	Possible out of bounds read due to incorrect validation of incoming buffer length in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile CVE ID : CVE-2021-1930	https://www. qualcomm.co m/company/ product- security/bull etins/august- 2021-bulletin	0-QUA-SA81- 200921/3166
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	08-Sep-21	10	Possible buffer overflow due to improper validation of device types during P2P search in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music,	https://www. qualcomm.co m/company/ product- security/bull etins/august- 2021-bulletin	0-QUA-SA81- 200921/3167

0-1 1-2

5-6

6-7

7-8

8-9

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID			
			Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking					
			CVE ID : CVE-2021-1972					
sa8155p_firm	nware							
Exposure of Resource to Wrong Sphere	08-Sep-21	2.1	Child process can leak information from parent process due to numeric pids are getting compared and these pid can be reused in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables CVE ID : CVE-2021-1904	https://www. qualcomm.co m/company/ product- security/bull etins/august- 2021-bulletin	0-QUA-SA81- 200921/3168			
Loop with Unreachable Exit Condition ('Infinite Loop')	08-Sep-21	5	Loop with unreachable exit condition may occur due to improper handling of unsupported input in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Voice & Music, Snapdragon Wearables CVE ID : CVE-2021-1914	https://www. qualcomm.co m/company/ product- security/bull etins/august- 2021-bulletin	O-QUA-SA81- 200921/3169			
Out-of- bounds Write	08-Sep-21	10	Possible buffer underflow due to lack of check for negative indices values when processing user provided input in Snapdragon Auto,	https://www. qualcomm.co m/company/ product- security/bull	O-QUA-SA81- 200921/3170			
CVSS Scoring Sc	ale 0-1	1-2	2-3 3-4 4-5 5-6	6-7 7-8	8-9 9-10			

Page 1230 of 1474

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Voice & Music, Snapdragon Wearables	etins/august- 2021-bulletin	
			CVE ID : CVE-2021-1916		
Integer Underflow (Wrap or Wraparoun d)	08-Sep-21	10	Integer underflow can occur when the RTCP length is lesser than than the actual blocks present in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Voice & Music, Snapdragon Wearables CVE ID : CVE-2021-1919	https://www. qualcomm.co m/company/ product- security/bull etins/august- 2021-bulletin	O-QUA-SA81- 200921/3171
Integer Underflow (Wrap or Wraparoun d)	08-Sep-21	10	Integer underflow can occur due to improper handling of incoming RTCP packets in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Voice & Music, Snapdragon Wearables CVE ID : CVE-2021-1920	https://www. qualcomm.co m/company/ product- security/bull etins/august- 2021-bulletin	0-QUA-SA81- 200921/3172
Incorrect Type Conversion or Cast	08-Sep-21	4.6	Incorrect pointer argument passed to trusted application TA could result in un- intended memory operations in Snapdragon Auto, Snapdragon Compute,	https://www. qualcomm.co m/company/ product- security/bull etins/august-	0-QUA-SA81- 200921/3173

0-1

5-6

6-7

7-8

8-9

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Snapdragon Connectivity, Snapdragon Industrial IOT CVE ID : CVE-2021-1923	2021-bulletin	
Exposure of Resource to Wrong Sphere	08-Sep-21	2.1	Lack of strict validation of bootmode can lead to information disclosure in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wearables CVE ID : CVE-2021-1929	https://www. qualcomm.co m/company/ product- security/bull etins/august- 2021-bulletin	0-QUA-SA81- 200921/3174
Improper Restriction of Operations within the Bounds of a Memory Buffer	08-Sep-21	3.6	Possible out of bounds read due to incorrect validation of incoming buffer length in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile CVE ID : CVE-2021-1930	https://www. qualcomm.co m/company/ product- security/bull etins/august- 2021-bulletin	0-QUA-SA81- 200921/3175
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	08-Sep-21	10	Possible buffer overflow due to improper validation of device types during P2P search in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Woice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking	https://www. qualcomm.co m/company/ product- security/bull etins/august- 2021-bulletin	O-QUA-SA81- 200921/3176
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 & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2021-1972		
sa8155_firm	ware			I	
Exposure of Resource to Wrong Sphere	08-Sep-21	2.1	Child process can leak information from parent process due to numeric pids are getting compared and these pid can be reused in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wearables CVE ID : CVE-2021-1904	https://www. qualcomm.co m/company/ product- security/bull etins/august- 2021-bulletin	0-QUA-SA81- 200921/3177
Loop with Unreachable Exit Condition ('Infinite Loop')	08-Sep-21	5	Loop with unreachable exit condition may occur due to improper handling of unsupported input in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Voice & Music, Snapdragon Wearables CVE ID : CVE-2021-1914	https://www. qualcomm.co m/company/ product- security/bull etins/august- 2021-bulletin	0-QUA-SA81- 200921/3178
Out-of- bounds Write	08-Sep-21	10	Possible buffer underflow due to lack of check for negative indices values when processing user provided input in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT,	https://www. qualcomm.co m/company/ product- security/bull etins/august- 2021-bulletin	0-QUA-SA81- 200921/3179

0-1

1-2

2-3 3-4 4-5 Page 1233 of 1474 5-6

6-7

7-8

8-9

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Snapdragon IoT, Snapdragon Voice & Music, Snapdragon Wearables		
			CVE ID : CVE-2021-1916		
Integer Underflow (Wrap or Wraparoun d)	08-Sep-21	10	Integer underflow can occur when the RTCP length is lesser than than the actual blocks present in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Voice & Music, Snapdragon Wearables CVE ID : CVE-2021-1919	https://www. qualcomm.co m/company/ product- security/bull etins/august- 2021-bulletin	O-QUA-SA81- 200921/3180
Integer Underflow (Wrap or Wraparoun d)	08-Sep-21	10	Integer underflow can occur due to improper handling of incoming RTCP packets in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Voice & Music, Snapdragon Wearables CVE ID : CVE-2021-1920	https://www. qualcomm.co m/company/ product- security/bull etins/august- 2021-bulletin	0-QUA-SA81- 200921/3181
Incorrect Type Conversion or Cast	08-Sep-21	4.6	Incorrect pointer argument passed to trusted application TA could result in un- intended memory operations in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Industrial IOT CVE ID : CVE-2021-1923	https://www. qualcomm.co m/company/ product- security/bull etins/august- 2021-bulletin	O-QUA-SA81- 200921/3182

CVSS Scoring Scale	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10
			D -	1224	- 6 4 4 7 4					

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Exposure of Resource to Wrong Sphere	08-Sep-21	2.1	Lack of strict validation of bootmode can lead to information disclosure in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wearables CVE ID : CVE-2021-1929	https://www. qualcomm.co m/company/ product- security/bull etins/august- 2021-bulletin	0-QUA-SA81- 200921/3183
Improper Restriction of Operations within the Bounds of a Memory Buffer	08-Sep-21	3.6	Possible out of bounds read due to incorrect validation of incoming buffer length in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile CVE ID : CVE-2021-1930	https://www. qualcomm.co m/company/ product- security/bull etins/august- 2021-bulletin	0-QUA-SA81- 200921/3184
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	08-Sep-21	10	Possible buffer overflow due to improper validation of device types during P2P search in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Woice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking CVE ID : CVE-2021-1972	https://www. qualcomm.co m/company/ product- security/bull etins/august- 2021-bulletin	0-QUA-SA81- 200921/3185
sa8195p_firm	nware				<u> </u>
Exposure of	08-Sep-21	2.1	Child process can leak	https://www.	0-QUA-SA81-
CVSS Scoring Sc	ale 0-1	1-2	2-3 3-4 4-5 5-6 Page 1235 of 1474	6-7 7-8	8-9 <mark>9-10</mark>

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Resource to Wrong Sphere			information from parent process due to numeric pids are getting compared and these pid can be reused in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wearables CVE ID : CVE-2021-1904	qualcomm.co m/company/ product- security/bull etins/august- 2021-bulletin	200921/3186
Out-of- bounds Write	08-Sep-21	10	Possible buffer underflow due to lack of check for negative indices values when processing user provided input in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Voice & Music, Snapdragon Wearables CVE ID : CVE-2021-1916	https://www. qualcomm.co m/company/ product- security/bull etins/august- 2021-bulletin	O-QUA-SA81- 200921/3187
Incorrect Type Conversion or Cast	08-Sep-21	4.6	Incorrect pointer argument passed to trusted application TA could result in un- intended memory operations in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Industrial IOT CVE ID : CVE-2021-1923	https://www. qualcomm.co m/company/ product- security/bull etins/august- 2021-bulletin	O-QUA-SA81- 200921/3188
Exposure of Resource to Wrong	08-Sep-21	2.1	Lack of strict validation of bootmode can lead to information disclosure in	https://www. qualcomm.co m/company/	O-QUA-SA81- 200921/3189

0-1

1-2

2-3 3-4

Page 1236 of 1474

4-5

5-6

6-7

7-8

8-9

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID			
Sphere			Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wearables CVE ID : CVE-2021-1929	product- security/bull etins/august- 2021-bulletin				
Improper Restriction of Operations within the Bounds of a Memory Buffer	08-Sep-21	3.6	Possible out of bounds read due to incorrect validation of incoming buffer length in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile	https://www. qualcomm.co m/company/ product- security/bull etins/august- 2021-bulletin	0-QUA-SA81- 200921/3190			
			CVE ID : CVE-2021-1930					
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	08-Sep-21	10	Possible buffer overflow due to improper validation of device types during P2P search in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Industrial IOT, Snapdragon Woice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking CVE ID : CVE-2021-1972	https://www. qualcomm.co m/company/ product- security/bull etins/august- 2021-bulletin	0-QUA-SA81- 200921/3191			
sc8180x_firmware								
Loop with Unreachable Exit Condition	08-Sep-21	5	Loop with unreachable exit condition may occur due to improper handling of unsupported input in	https://www. qualcomm.co m/company/ product-	0-QUA-SC81- 200921/3192			
CVSS Scoring Sca	ale 0-1	1-2	2-3 3-4 4-5 5-6	6-7 7-8	8-9 <mark>9-10</mark>			

Page 1237 of 1474

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
('Infinite Loop')			Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Voice & Music, Snapdragon Wearables CVE ID : CVE-2021-1914	security/bull etins/august- 2021-bulletin	
Out-of- bounds Write	08-Sep-21	10	Possible buffer underflow due to lack of check for negative indices values when processing user provided input in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Voice & Music, Snapdragon Wearables CVE ID : CVE-2021-1916	https://www. qualcomm.co m/company/ product- security/bull etins/august- 2021-bulletin	0-QUA-SC81- 200921/3193
Integer Underflow (Wrap or Wraparoun d)	08-Sep-21	10	Integer underflow can occur when the RTCP length is lesser than than the actual blocks present in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Voice & Music, Snapdragon Wearables CVE ID : CVE-2021-1919	https://www. qualcomm.co m/company/ product- security/bull etins/august- 2021-bulletin	O-QUA-SC81- 200921/3194
Integer Underflow (Wrap or Wraparoun	08-Sep-21	10	Integer underflow can occur due to improper handling of incoming RTCP packets in Snapdragon Auto,	https://www. qualcomm.co m/company/ product-	0-QUA-SC81- 200921/3195

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
d)			Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Voice & Music, Snapdragon Wearables CVE ID : CVE-2021-1920	security/bull etins/august- 2021-bulletin	
sd205_firmw	are				
Exposure of Resource to Wrong Sphere	08-Sep-21	2.1	Child process can leak information from parent process due to numeric pids are getting compared and these pid can be reused in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables CVE ID : CVE-2021-1904	https://www. qualcomm.co m/company/ product- security/bull etins/august- 2021-bulletin	0-QUA-SD20- 200921/3196
Loop with Unreachable Exit Condition ('Infinite Loop')	08-Sep-21	5	Loop with unreachable exit condition may occur due to improper handling of unsupported input in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Voice & Music, Snapdragon Wearables CVE ID : CVE-2021-1914	https://www. qualcomm.co m/company/ product- security/bull etins/august- 2021-bulletin	0-QUA-SD20- 200921/3197
Out-of- bounds	08-Sep-21	10	Possible buffer underflow due to lack of check for	https://www. qualcomm.co	0-QUA-SD20- 200921/3198

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Write			negative indices values when processing user provided input in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Voice & Music, Snapdragon Wearables CVE ID : CVE-2021-1916	m/company/ product- security/bull etins/august- 2021-bulletin	
Integer Underflow (Wrap or Wraparoun d)	08-Sep-21	10	Integer underflow can occur when the RTCP length is lesser than than the actual blocks present in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Voice & Music, Snapdragon Wearables CVE ID : CVE-2021-1919	https://www. qualcomm.co m/company/ product- security/bull etins/august- 2021-bulletin	0-QUA-SD20- 200921/3199
Integer Underflow (Wrap or Wraparoun d)	08-Sep-21	10	Integer underflow can occur due to improper handling of incoming RTCP packets in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Voice & Music, Snapdragon Wearables CVE ID : CVE-2021-1920	https://www. qualcomm.co m/company/ product- security/bull etins/august- 2021-bulletin	O-QUA-SD20- 200921/3200
Out-of- bounds Read	08-Sep-21	3.6	Buffer over read could occur due to incorrect check of buffer size while flashing	https://www. qualcomm.co m/company/	0-QUA-SD20- 200921/3201

 3-4
 4-5

 Page 1240 of 1474

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			emmc devices in Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking CVE ID : CVE-2021-1928	product- security/bull etins/august- 2021-bulletin	
Exposure of Resource to Wrong Sphere	08-Sep-21	2.1	Lack of strict validation of bootmode can lead to information disclosure in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wearables CVE ID : CVE-2021-1929	https://www. qualcomm.co m/company/ product- security/bull etins/august- 2021-bulletin	0-QUA-SD20- 200921/3202
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	08-Sep-21	10	Possible buffer overflow due to improper validation of device types during P2P search in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Industrial IOT, Snapdragon Woile, Snapdragon Woice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking CVE ID : CVE-2021-1972	https://www. qualcomm.co m/company/ product- security/bull etins/august- 2021-bulletin	O-QUA-SD20- 200921/3203
sd210_firmw	/are				
Exposure of	08-Sep-21	2.1	Child process can leak	https://www.	0-QUA-SD21-
CVSS Scoring Sc	cale 0-1	1-2	2-3 3-4 4-5 5-6 Page 1241 of 1474	6-7 7-8	8-9 9-10

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Resource to Wrong Sphere			information from parent process due to numeric pids are getting compared and these pid can be reused in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wearables CVE ID : CVE-2021-1904	qualcomm.co m/company/ product- security/bull etins/august- 2021-bulletin	200921/3204
Loop with Unreachable Exit Condition ('Infinite Loop')	08-Sep-21	5	Loop with unreachable exit condition may occur due to improper handling of unsupported input in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Voice & Music, Snapdragon Wearables CVE ID : CVE-2021-1914	https://www. qualcomm.co m/company/ product- security/bull etins/august- 2021-bulletin	0-QUA-SD21- 200921/3205
Out-of- bounds Write	08-Sep-21	10	Possible buffer underflow due to lack of check for negative indices values when processing user provided input in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Voice & Music, Snapdragon Wearables	https://www. qualcomm.co m/company/ product- security/bull etins/august- 2021-bulletin	0-QUA-SD21- 200921/3206

C	VSS Scoring Scale	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10
				Pa	age 1242 (of 1474					

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2021-1916		
Integer Underflow (Wrap or Wraparoun d)	08-Sep-21	10	Integer underflow can occur when the RTCP length is lesser than than the actual blocks present in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Voice & Music, Snapdragon Wearables CVE ID : CVE-2021-1919	https://www. qualcomm.co m/company/ product- security/bull etins/august- 2021-bulletin	0-QUA-SD21- 200921/3207
Integer Underflow (Wrap or Wraparoun d)	08-Sep-21	10	Integer underflow can occur due to improper handling of incoming RTCP packets in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Voice & Music, Snapdragon Wearables	https://www. qualcomm.co m/company/ product- security/bull etins/august- 2021-bulletin	O-QUA-SD21- 200921/3208
			CVE ID : CVE-2021-1920		
Out-of- bounds Read	08-Sep-21	3.6	Buffer over read could occur due to incorrect check of buffer size while flashing emmc devices in Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking	https://www. qualcomm.co m/company/ product- security/bull etins/august- 2021-bulletin	0-QUA-SD21- 200921/3209
			CVE ID : CVE-2021-1928		
CVSS Scoring Sco	ale 0-1	1-2	2-3 3-4 4-5 5-6	6-7 7-8	8-9 9-10
			Page 1243 of 1474		

Exposure of Resource to Wrong Sphere08-Sep-21Snapdragon Auto, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Mobile, Snapdragon Wearablesn/c mode secu etime 2021SubfereVVE ID: CVE-2021-1929	C	e	CVSS	Description & CVE ID	Patch	NCIIPC ID
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')08-Sep-2110Snapdragon Compute, Snapdragon Consumer IOT, Snapdragon Consumer IOT, Snapdragon Mobile, Snapdragon Mobile, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networkingetime secu Snapdragon Wired Infrastructure and Networkingsd429_firmExposure of Resource to Wrong Sphere08-Sep-21Child process can leak information from parent process due to numeric pids are getting compared and these pid can be reused in Snapdragon Consumer IOT, Snapdragon Consumer IOT, Snapdragon Consumer IOT, process due to numeric pids are getting compared and these pid can be reused in Snapdragon Consumer IOT, Snapdragon Consumer IOT, Snapdragon Consumer IOT, sonapdragon Consumer IOT, process compared and these pid can be reused in Snapdragon Consumer IOT, Snapdragon Consumer IOT, Sna	2		2.1	bootmode can lead to information disclosure in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wearables	https://www. qualcomm.co m/company/ product- security/bull etins/august- 2021-bulletin	0-QUA-SD21- 200921/3210
Exposure of Resource to Wrong Sphere08-Sep-212.1Child process can leak information from parent process due to numeric pids these pid can be reused in Snapdragon Compute, Snapdragon Consumer IOT,httpsExposure of Resource to Wrong Sphere08-Sep-212.1Snapdragon Connectivity, Snapdragon Consumer IOT, 2022	1		10	to improper validation of device types during P2P search in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Woice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking	https://www. qualcomm.co m/company/ product- security/bull etins/august- 2021-bulletin	0-QUA-SD21- 200921/3211
Exposure of Resource to Wrong Sphere08-Sep-212.1information from parent process due to numeric pids are getting compared and these pid can be reused in Snapdragon Auto, Snapdragon Connectivity, Snapdragon Consumer IOT,https: qual m/ce secu state		_				
Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music,	xposure of esource to Yrong 08-Sep-21 2.1		2.1	information from parent process due to numeric pids are getting compared and these pid can be reused in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile,	https://www. qualcomm.co m/company/ product- security/bull etins/august- 2021-bulletin	0-QUA-SD42- 200921/3212

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Snapdragon Wearables		
			CVE ID : CVE-2021-1904		
Loop with Unreachable Exit Condition ('Infinite Loop')	08-Sep-21	5	Loop with unreachable exit condition may occur due to improper handling of unsupported input in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Voice & Music, Snapdragon Wearables	https://www. qualcomm.co m/company/ product- security/bull etins/august- 2021-bulletin	0-QUA-SD42- 200921/3213
			CVE ID : CVE-2021-1914		
Out-of- bounds Write	08-Sep-21	10	Possible buffer underflow due to lack of check for negative indices values when processing user provided input in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Voice & Music, Snapdragon Wearables	https://www. qualcomm.co m/company/ product- security/bull etins/august- 2021-bulletin	0-QUA-SD42- 200921/3214
			CVE ID : CVE-2021-1916		
Integer Underflow (Wrap or Wraparoun d)	08-Sep-21	10	Integer underflow can occur when the RTCP length is lesser than than the actual blocks present in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Voice & Music, Snapdragon	https://www. qualcomm.co m/company/ product- security/bull etins/august- 2021-bulletin	O-QUA-SD42- 200921/3215

0-1

1-2

2-3 3-4 4-5 Page 1245 of 1474 5-6

6-7

7-8

8-9

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Wearables		
			CVE ID : CVE-2021-1919		
Integer Underflow (Wrap or Wraparoun d)	08-Sep-21	10	Integer underflow can occur due to improper handling of incoming RTCP packets in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Voice & Music, Snapdragon Wearables	https://www. qualcomm.co m/company/ product- security/bull etins/august- 2021-bulletin	0-QUA-SD42- 200921/3216
			CVE ID : CVE-2021-1920		
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	08-Sep-21	10	Possible buffer overflow due to improper validation of device types during P2P search in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Woice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking CVE ID : CVE-2021-1972	https://www. qualcomm.co m/company/ product- security/bull etins/august- 2021-bulletin	0-QUA-SD42- 200921/3217
sd439_firmw	are				
Exposure of Resource to Wrong Sphere	08-Sep-21	2.1	Child process can leak information from parent process due to numeric pids are getting compared and these pid can be reused in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity,	https://www. qualcomm.co m/company/ product- security/bull etins/august- 2021-bulletin	0-QUA-SD43- 200921/3218
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 & CVE ID	Patch	NCIIPC ID
			Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables CVE ID : CVE-2021-1904		
Loop with Unreachable Exit Condition ('Infinite Loop')	08-Sep-21	5	Loop with unreachable exit condition may occur due to improper handling of unsupported input in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Voice & Music, Snapdragon Wearables CVE ID : CVE-2021-1914	https://www. qualcomm.co m/company/ product- security/bull etins/august- 2021-bulletin	0-QUA-SD43- 200921/3219
Out-of- bounds Write	08-Sep-21	10	Possible buffer underflow due to lack of check for negative indices values when processing user provided input in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Voice & Music, Snapdragon Wearables CVE ID : CVE-2021-1916	https://www. qualcomm.co m/company/ product- security/bull etins/august- 2021-bulletin	0-QUA-SD43- 200921/3220
Integer Underflow (Wrap or Wraparoun d)	08-Sep-21	10	Integer underflow can occur when the RTCP length is lesser than than the actual blocks present in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity,	https://www. qualcomm.co m/company/ product- security/bull etins/august-	0-QUA-SD43- 200921/3221

0-1

1-2 2-3

4-5

5-6

6-7

7-8

8-9

9-10

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Voice & Music, Snapdragon Wearables CVE ID : CVE-2021-1919	2021-bulletin	
Integer Underflow (Wrap or Wraparoun d)	08-Sep-21	10	Integer underflow can occur due to improper handling of incoming RTCP packets in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Voice & Music, Snapdragon Wearables	https://www. qualcomm.co m/company/ product- security/bull etins/august- 2021-bulletin	0-QUA-SD43- 200921/3222
			CVE ID : CVE-2021-1920		
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	08-Sep-21	10	Possible buffer overflow due to improper validation of device types during P2P search in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Woice & Music, Snapdragon Wired Infrastructure and Networking CVE ID : CVE-2021-1972	https://www. qualcomm.co m/company/ product- security/bull etins/august- 2021-bulletin	0-QUA-SD43- 200921/3223
sd450_firmware					
Exposure of Resource to Wrong Sphere	08-Sep-21	2.1	Child process can leak information from parent process due to numeric pids are getting compared and	https://www. qualcomm.co m/company/ product-	0-QUA-SD45- 200921/3224
CVSS Scoring Sc	ale 0-1	1-2	2-3 3-4 4-5 5-6 Page 1248 of 1474	6-7 7-8	8-9 9-10

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			these pid can be reused in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables CVE ID : CVE-2021-1904	security/bull etins/august- 2021-bulletin	
Loop with Unreachable Exit Condition ('Infinite Loop')	08-Sep-21	5	Loop with unreachable exit condition may occur due to improper handling of unsupported input in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Voice & Music, Snapdragon Wearables CVE ID : CVE-2021-1914	https://www. qualcomm.co m/company/ product- security/bull etins/august- 2021-bulletin	O-QUA-SD45- 200921/3225
Out-of- bounds Write	08-Sep-21	10	Possible buffer underflow due to lack of check for negative indices values when processing user provided input in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Voice & Music, Snapdragon Wearables CVE ID : CVE-2021-1916	https://www. qualcomm.co m/company/ product- security/bull etins/august- 2021-bulletin	0-QUA-SD45- 200921/3226
Integer Underflow	08-Sep-21	10	Integer underflow can occur when the RTCP length is	https://www. qualcomm.co	0-QUA-SD45- 200921/3227
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 & CVE ID	Patch	NCIIPC ID
(Wrap or Wraparoun d)			lesser than than the actual blocks present in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Voice & Music, Snapdragon Wearables CVE ID : CVE-2021-1919	m/company/ product- security/bull etins/august- 2021-bulletin	
Integer Underflow (Wrap or Wraparoun d)	08-Sep-21	10	Integer underflow can occur due to improper handling of incoming RTCP packets in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Voice & Music, Snapdragon Wearables CVE ID : CVE-2021-1920	https://www. qualcomm.co m/company/ product- security/bull etins/august- 2021-bulletin	0-QUA-SD45- 200921/3228
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	08-Sep-21	10	Possible buffer overflow due to improper validation of device types during P2P search in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Woice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking	https://www. qualcomm.co m/company/ product- security/bull etins/august- 2021-bulletin	0-QUA-SD45- 200921/3229
cd460 firmer	ara		CVE ID : CVE-2021-1972		
sd460_firmw	are				
CVSS Scoring Sca	ale 0-1	1-2	2-3 3-4 4-5 5-6 Page 1250 of 1474	6-7 7-8	8-9 9-10

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Exposure of Resource to Wrong Sphere	08-Sep-21	2.1	Child process can leak information from parent process due to numeric pids are getting compared and these pid can be reused in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables CVE ID : CVE-2021-1904	https://www. qualcomm.co m/company/ product- security/bull etins/august- 2021-bulletin	0-QUA-SD46- 200921/3230
Incorrect Type Conversion or Cast	08-Sep-21	4.6	Incorrect pointer argument passed to trusted application TA could result in un- intended memory operations in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Industrial IOT CVE ID : CVE-2021-1923	https://www. qualcomm.co m/company/ product- security/bull etins/august- 2021-bulletin	0-QUA-SD46- 200921/3231
Exposure of Resource to Wrong Sphere	08-Sep-21	2.1	Lack of strict validation of bootmode can lead to information disclosure in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wearables CVE ID : CVE-2021-1929	https://www. qualcomm.co m/company/ product- security/bull etins/august- 2021-bulletin	0-QUA-SD46- 200921/3232
Improper Restriction of Operations	08-Sep-21	3.6	Possible out of bounds read due to incorrect validation of incoming buffer length in Snapdragon Auto,	https://www. qualcomm.co m/company/ product-	0-QUA-SD46- 200921/3233

CVSS Scoring Scale	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10
			Da	a 1251	of 1 1 7 1					

Page 1251 of 1474

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
within the Bounds of a Memory Buffer			Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile	security/bull etins/august- 2021-bulletin	
			CVE ID : CVE-2021-1930		
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	08-Sep-21	10	Possible buffer overflow due to improper validation of device types during P2P search in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Woice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking CVE ID : CVE-2021-1972	https://www. qualcomm.co m/company/ product- security/bull etins/august- 2021-bulletin	0-QUA-SD46- 200921/3234
sd480_firmw	are		CVE ID . CVE-2021-1972		
Exposure of Resource to Wrong Sphere	08-Sep-21	2.1	Child process can leak information from parent process due to numeric pids are getting compared and these pid can be reused in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wearables CVE ID : CVE-2021-1904	https://www. qualcomm.co m/company/ product- security/bull etins/august- 2021-bulletin	0-QUA-SD48- 200921/3235
Loop with Unreachable	08-Sep-21	5	Loop with unreachable exit condition may occur due to	https://www. qualcomm.co	0-QUA-SD48- 200921/3236

Page 1252 of 1474

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Exit Condition ('Infinite Loop')			improper handling of unsupported input in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Voice & Music, Snapdragon Wearables CVE ID : CVE-2021-1914	m/company/ product- security/bull etins/august- 2021-bulletin	
Out-of- bounds Write	08-Sep-21	10	Possible buffer underflow due to lack of check for negative indices values when processing user provided input in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Voice & Music, Snapdragon Wearables CVE ID : CVE-2021-1916	https://www. qualcomm.co m/company/ product- security/bull etins/august- 2021-bulletin	0-QUA-SD48- 200921/3237
Integer Underflow (Wrap or Wraparoun d)	08-Sep-21	10	Integer underflow can occur when the RTCP length is lesser than than the actual blocks present in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Voice & Music, Snapdragon Wearables CVE ID : CVE-2021-1919	https://www. qualcomm.co m/company/ product- security/bull etins/august- 2021-bulletin	0-QUA-SD48- 200921/3238
Integer	08-Sep-21	10	Integer underflow can occur due to improper handling of	https://www. qualcomm.co	0-QUA-SD48- 200921/3239

 3-4
 4-5
 5-6
 6-7

 Page 1253 of 1474

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
(Wrap or Wraparoun d)			incoming RTCP packets in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Voice & Music, Snapdragon Wearables CVE ID : CVE-2021-1920	m/company/ product- security/bull etins/august- 2021-bulletin	
Incorrect Type Conversion or Cast	08-Sep-21	4.6	Incorrect pointer argument passed to trusted application TA could result in un- intended memory operations in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Industrial IOT CVE ID : CVE-2021-1923	https://www. qualcomm.co m/company/ product- security/bull etins/august- 2021-bulletin	0-QUA-SD48- 200921/3240
Exposure of Resource to Wrong Sphere	08-Sep-21	2.1	Lack of strict validation of bootmode can lead to information disclosure in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wearables CVE ID : CVE-2021-1929	https://www. qualcomm.co m/company/ product- security/bull etins/august- 2021-bulletin	0-QUA-SD48- 200921/3241
Improper Restriction of Operations within the Bounds of a Memory Buffer	08-Sep-21	3.6	Possible out of bounds read due to incorrect validation of incoming buffer length in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT,	https://www. qualcomm.co m/company/ product- security/bull etins/august- 2021-bulletin	0-QUA-SD48- 200921/3242

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Snapdragon Mobile CVE ID : CVE-2021-1930		
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	08-Sep-21	10	Possible buffer overflow due to improper validation of device types during P2P search in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Woice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking CVE ID : CVE-2021-1972	https://www. qualcomm.co m/company/ product- security/bull etins/august- 2021-bulletin	0-QUA-SD48- 200921/3243
sd632_firmw	are				
Exposure of Resource to Wrong Sphere	xposure of esource to Trong 08-Sep-21 2.1		Child process can leak information from parent process due to numeric pids are getting compared and these pid can be reused in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wearables CVE ID : CVE-2021-1904	https://www. qualcomm.co m/company/ product- security/bull etins/august- 2021-bulletin	0-QUA-SD63- 200921/3244
Loop with Unreachable Exit Condition ('Infinite Loop')	08-Sep-21	5	Loop with unreachable exit condition may occur due to improper handling of unsupported input in Snapdragon Auto, Snapdragon Compute,	https://www. qualcomm.co m/company/ product- security/bull etins/august-	0-QUA-SD63- 200921/3245

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Voice & Music, Snapdragon Wearables CVE ID : CVE-2021-1914	2021-bulletin	
Out-of- bounds Write	08-Sep-21	10	Possible buffer underflow due to lack of check for negative indices values when processing user provided input in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Voice & Music, Snapdragon Wearables CVE ID : CVE-2021-1916	https://www. qualcomm.co m/company/ product- security/bull etins/august- 2021-bulletin	0-QUA-SD63- 200921/3246
Integer Underflow (Wrap or Wraparoun d)	08-Sep-21	10	Integer underflow can occur when the RTCP length is lesser than than the actual blocks present in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Voice & Music, Snapdragon Wearables CVE ID : CVE-2021-1919	https://www. qualcomm.co m/company/ product- security/bull etins/august- 2021-bulletin	0-QUA-SD63- 200921/3247
Integer Underflow (Wrap or Wraparoun d)	08-Sep-21	10	Integer underflow can occur due to improper handling of incoming RTCP packets in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity,	https://www. qualcomm.co m/company/ product- security/bull etins/august-	0-QUA-SD63- 200921/3248

0-1

1-2

5-6

6-7

7-8

8-9

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID	
			Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Voice & Music, Snapdragon Wearables CVE ID : CVE-2021-1920	2021-bulletin		
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	08-Sep-21	10	Possible buffer overflow due to improper validation of device types during P2P search in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Woice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking CVE ID : CVE-2021-1972	https://www. qualcomm.co m/company/ product- security/bull etins/august- 2021-bulletin	0-QUA-SD63- 200921/3249	
sd660_firmw	are					
Exposure of Resource to Wrong Sphere	08-Sep-21	2.1	Child process can leak information from parent process due to numeric pids are getting compared and these pid can be reused in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wearables CVE ID : CVE-2021-1904	https://www. qualcomm.co m/company/ product- security/bull etins/august- 2021-bulletin	0-QUA-SD66- 200921/3250	
Buffer Copy without	08-Sep-21	10	Possible buffer overflow due to improper validation of	https://www. qualcomm.co	0-QUA-SD66- 200921/3251	

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Checking Size of Input ('Classic Buffer Overflow')			device types during P2P search in Snapdragon Auto Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT Snapdragon Industrial IOT Snapdragon Mobile, Snapdragon Woice & Music Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking CVE ID : CVE-2021-1972	security/bull etins/august- Γ, 2021-bulletin Γ,	
sd662_firmw	are		CVE ID : CVE-2021-1972		
Exposure of Resource to Wrong Sphere	08-Sep-21	2.1	Child process can leak information from parent process due to numeric pic are getting compared and these pid can be reused in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT Snapdragon Industrial IOT Snapdragon Mobile, Snapdragon Wearables CVE ID : CVE-2021-1904	https://www. qualcomm.co m/company/ product- security/bull etins/august- 2021-bulletin	0-QUA-SD66- 200921/3252
Incorrect Type Conversion or Cast	08-Sep-21	4.6	Incorrect pointer argumer passed to trusted applicate TA could result in un- intended memory operatio in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Industrial IOT CVE ID : CVE-2021-1923	ion https://www. qualcomm.co m/company/ product- security/bull etins/august-	0-QUA-SD66- 200921/3253
Exposure of	08-Sep-21	2.1	Lack of strict validation of	https://www.	0-QUA-SD66-
CVSS Scoring Sc	ale 0-1	1-2	2-3 3-4 4-5 5	5-6 6-7 7-8	8-9 9-10

Page 1258 of 1474

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID		
Resource to Wrong Sphere			bootmode can lead to information disclosure in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wearables CVE ID : CVE-2021-1929	qualcomm.co m/company/ product- security/bull etins/august- 2021-bulletin	200921/3254		
Improper Restriction of Operations within the Bounds of a Memory Buffer	08-Sep-21	3.6	Possible out of bounds read due to incorrect validation of incoming buffer length in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile CVE ID : CVE-2021-1930	https://www. qualcomm.co m/company/ product- security/bull etins/august- 2021-bulletin	0-QUA-SD66- 200921/3255		
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	08-Sep-21	10	Possible buffer overflow due to improper validation of device types during P2P search in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Industrial IOT, Snapdragon Woile, Snapdragon Woice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking CVE ID : CVE-2021-1972	https://www. qualcomm.co m/company/ product- security/bull etins/august- 2021-bulletin	0-QUA-SD66- 200921/3256		
sd665_firmware							
Exposure of Resource to	08-Sep-21	2.1	Child process can leak information from parent	https://www. qualcomm.co	0-QUA-SD66- 200921/3257		
CVSS Scoring Sc	ale 0-1	1-2	2-3 3-4 4-5 5-6 Page 1259 of 1474	6-7 7-8	8-9 9-10		

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Wrong Sphere			process due to numeric pids are getting compared and these pid can be reused in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables CVE ID : CVE-2021-1904	m/company/ product- security/bull etins/august- 2021-bulletin	
Loop with Unreachable Exit Condition ('Infinite Loop')	08-Sep-21	5	Loop with unreachable exit condition may occur due to improper handling of unsupported input in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Voice & Music, Snapdragon Wearables CVE ID : CVE-2021-1914	https://www. qualcomm.co m/company/ product- security/bull etins/august- 2021-bulletin	0-QUA-SD66- 200921/3258
Out-of- bounds Write	08-Sep-21	10	Possible buffer underflow due to lack of check for negative indices values when processing user provided input in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Voice & Music, Snapdragon Wearables CVE ID : CVE-2021-1916	https://www. qualcomm.co m/company/ product- security/bull etins/august- 2021-bulletin	0-QUA-SD66- 200921/3259

CVSS Scoring Scale	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9
			Ра	ige 1260	of 1474				

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Integer Underflow (Wrap or Wraparoun d)	08-Sep-21	10	Integer underflow can occur when the RTCP length is lesser than than the actual blocks present in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Voice & Music, Snapdragon Wearables	https://www. qualcomm.co m/company/ product- security/bull etins/august- 2021-bulletin	O-QUA-SD66- 200921/3260
			CVE ID : CVE-2021-1919		
Integer Underflow (Wrap or Wraparoun d)	08-Sep-21	10	Integer underflow can occur due to improper handling of incoming RTCP packets in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Voice & Music, Snapdragon Wearables	https://www. qualcomm.co m/company/ product- security/bull etins/august- 2021-bulletin	O-QUA-SD66- 200921/3261
			CVE ID : CVE-2021-1920		
Incorrect Type Conversion or Cast	08-Sep-21	4.6	Incorrect pointer argument passed to trusted application TA could result in un- intended memory operations in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Industrial IOT CVE ID : CVE-2021-1923	https://www. qualcomm.co m/company/ product- security/bull etins/august- 2021-bulletin	0-QUA-SD66- 200921/3262
Exposure of Resource to Wrong Sphere	08-Sep-21	2.1	Lack of strict validation of bootmode can lead to information disclosure in Snapdragon Auto, Snapdragon Compute,	https://www. qualcomm.co m/company/ product- security/bull	0-QUA-SD66- 200921/3263

1-2

0-1

5-6

6-7

7-8

8-9

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wearables	etins/august- 2021-bulletin	
			CVE ID : CVE-2021-1929		
Improper Restriction of Operations within the Bounds of a Memory Buffer	08-Sep-21	3.6	Possible out of bounds read due to incorrect validation of incoming buffer length in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile	https://www. qualcomm.co m/company/ product- security/bull etins/august- 2021-bulletin	0-QUA-SD66- 200921/3264
			CVE ID : CVE-2021-1930		
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	08-Sep-21	10	Possible buffer overflow due to improper validation of device types during P2P search in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Woice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking CVE ID : CVE-2021-1972	https://www. qualcomm.co m/company/ product- security/bull etins/august- 2021-bulletin	0-QUA-SD66- 200921/3265
sd670_firmw	are				
Exposure of Resource to Wrong Sphere	08-Sep-21	2.1	Child process can leak information from parent process due to numeric pids are getting compared and these pid can be reused in Snapdragon Auto,	https://www. qualcomm.co m/company/ product- security/bull etins/august-	0-QUA-SD67- 200921/3266
CVSS Scoring Sc	ale 0-1	1-2	2-3 3-4 4-5 5-6 Page 1262 of 1474	6-7 7-8	8-9 9-10

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables	2021-bulletin	
			CVE ID : CVE-2021-1904		
Loop with Unreachable Exit Condition ('Infinite Loop')	08-Sep-21	5	Loop with unreachable exit condition may occur due to improper handling of unsupported input in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Voice & Music, Snapdragon Wearables CVE ID : CVE-2021-1914	https://www. qualcomm.co m/company/ product- security/bull etins/august- 2021-bulletin	0-QUA-SD67- 200921/3267
Out-of- bounds Write	08-Sep-21	10	Possible buffer underflow due to lack of check for negative indices values when processing user provided input in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Voice & Music, Snapdragon Wearables CVE ID : CVE-2021-1916	https://www. qualcomm.co m/company/ product- security/bull etins/august- 2021-bulletin	0-QUA-SD67- 200921/3268
Integer Underflow (Wrap or Wraparoun	08-Sep-21	10	Integer underflow can occur when the RTCP length is lesser than than the actual blocks present in Snapdragon	https://www. qualcomm.co m/company/ product-	0-QUA-SD67- 200921/3269

CVSS Scoring Scale	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10
Page 1263 of 1474										

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
d)			Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Voice & Music, Snapdragon Wearables	security/bull etins/august- 2021-bulletin	
			CVE ID : CVE-2021-1919		
Integer Underflow (Wrap or Wraparoun d)	08-Sep-21	10	Integer underflow can occur due to improper handling of incoming RTCP packets in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Voice & Music, Snapdragon Wearables CVE ID : CVE-2021-1920	https://www. qualcomm.co m/company/ product- security/bull etins/august- 2021-bulletin	0-QUA-SD67- 200921/3270
Incorrect Type Conversion or Cast	08-Sep-21	4.6	Incorrect pointer argument passed to trusted application TA could result in un- intended memory operations in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Industrial IOT CVE ID : CVE-2021-1923	https://www. qualcomm.co m/company/ product- security/bull etins/august- 2021-bulletin	0-QUA-SD67- 200921/3271
Improper Restriction of Operations within the Bounds of a Memory Buffer	08-Sep-21	3.6	Possible out of bounds read due to incorrect validation of incoming buffer length in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile	https://www. qualcomm.co m/company/ product- security/bull etins/august- 2021-bulletin	0-QUA-SD67- 200921/3272

0-1

1-2

4-5

5-6

6-7

7-8

8-9

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2021-1930		
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	08-Sep-21	10	Possible buffer overflow due to improper validation of device types during P2P search in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Woice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking CVE ID : CVE-2021-1972	https://www. qualcomm.co m/company/ product- security/bull etins/august- 2021-bulletin	0-QUA-SD67- 200921/3273
sd675_firmw	are				
Exposure of Resource to Wrong Sphere	08-Sep-21	2.1	Child process can leak information from parent process due to numeric pids are getting compared and these pid can be reused in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wearables CVE ID : CVE-2021-1904	https://www. qualcomm.co m/company/ product- security/bull etins/august- 2021-bulletin	0-QUA-SD67- 200921/3274
Loop with Unreachable Exit Condition ('Infinite Loop')	08-Sep-21	5	Loop with unreachable exit condition may occur due to improper handling of unsupported input in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity,	https://www. qualcomm.co m/company/ product- security/bull etins/august- 2021-bulletin	0-QUA-SD67- 200921/3275
CVSS Scoring Sc	ale 0-1	1-2	2-3 3-4 4-5 5-6	6-7 7-8	8-9 9-10

 3-4
 4-5
 5-6
 6-7

 Page 1265 of 1474

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Voice & Music, Snapdragon Wearables CVE ID : CVE-2021-1914		
Out-of- bounds Write	08-Sep-21	10	Possible buffer underflow due to lack of check for negative indices values when processing user provided input in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Voice & Music, Snapdragon Wearables CVE ID : CVE-2021-1916	https://www. qualcomm.co m/company/ product- security/bull etins/august- 2021-bulletin	0-QUA-SD67- 200921/3276
Integer Underflow (Wrap or Wraparoun d)	08-Sep-21	10	Integer underflow can occur when the RTCP length is lesser than than the actual blocks present in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Voice & Music, Snapdragon Wearables CVE ID : CVE-2021-1919	https://www. qualcomm.co m/company/ product- security/bull etins/august- 2021-bulletin	0-QUA-SD67- 200921/3277
Integer Underflow (Wrap or Wraparoun d)	08-Sep-21	10	Integer underflow can occur due to improper handling of incoming RTCP packets in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT,	https://www. qualcomm.co m/company/ product- security/bull etins/august- 2021-bulletin	0-QUA-SD67- 200921/3278

		Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Voice & Music, Snapdragon Wearables		
		CVE ID : CVE-2021-1920		
08-Sep-21	4.6	Incorrect pointer argument passed to trusted application TA could result in un- intended memory operations in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Industrial IOT CVE ID : CVE-2021-1923	https://www. qualcomm.co m/company/ product- security/bull etins/august- 2021-bulletin	0-QUA-SD67- 200921/3279
08-Sep-21	2.1	Lack of strict validation of bootmode can lead to information disclosure in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wearables	https://www. qualcomm.co m/company/ product- security/bull etins/august- 2021-bulletin	0-QUA-SD67- 200921/3280
08-Sep-21	3.6	Possible out of bounds read due to incorrect validation of incoming buffer length in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile CVE ID : CVE-2021-1930	https://www. qualcomm.co m/company/ product- security/bull etins/august- 2021-bulletin	0-QUA-SD67- 200921/3281
08-Sep-21	10	Possible buffer overflow due to improper validation of device types during P2P	https://www. qualcomm.co m/company/	0-QUA-SD67- 200921/3282
	08-Sep-21 08-Sep-21	08-Sep-21 2.1 08-Sep-21 3.6 08-Sep-21 10	Noice & Music, Snapdragon WearablesCVE ID : CVE-2021-192008-Sep-21Incorrect pointer argument passed to trusted application TA could result in un- intended memory operations in Snapdragon Auto, Snapdragon Compute, Snapdragon Industrial IOT08-Sep-214.62.1Lack of strict validation of bootmode can lead to information disclosure in Snapdragon Compute, Snapdragon Compute, Snapdragon Auto, Snapdragon Auto, Snapdragon Industrial IOT08-Sep-212.108-Sep-21Sae08-Sep-21Sae08-Sep-21Sae08-Sep-21Sae08-Sep-21Sae08-Sep-21Sae08-Sep-21Sae08-Sep-21Sae08-Sep-21Possible out of bounds read due to incorrect validation of incoming buffer length in Snapdragon Compute, Snapdragon Compute, Snapdragon Compute, Snapdragon Auto, Snapdragon Auto, Snapdragon Compute, Snapdragon Industrial IOT, Snapdragon Industrial IO	Noice & Music, Snapdragon WearablesVoice & Music, Snapdragon WearablesCVE ID : CVE-2021-1920CVE ID : CVE-2021-192008-Sep-214.6Incorrect pointer argument passed to trusted application intended memory operations in Snapdragon Compute, Snapdragon Connectivity, Snapdragon Industrial IOT CVE ID : CVE-2021-1923https://www. qualcomm.co m/company/ product- security/bull etins/august- 2021-bulletin08-Sep-212.1Lack of strict validation of bootmode can lead to information disclosure in Snapdragon Conpute, Snapdragon Consumer IOT,

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Size of Input ('Classic Buffer Overflow')			search in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking CVE ID : CVE-2021-1972	product- security/bull etins/august- 2021-bulletin	
sd678_firmw	are				
Exposure of Resource to Wrong Sphere	08-Sep-21	2.1	Child process can leak information from parent process due to numeric pids are getting compared and these pid can be reused in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables CVE ID : CVE-2021-1904	https://www. qualcomm.co m/company/ product- security/bull etins/august- 2021-bulletin	0-QUA-SD67- 200921/3283
Loop with Unreachable Exit Condition ('Infinite Loop')	08-Sep-21	5	Loop with unreachable exit condition may occur due to improper handling of unsupported input in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Voice & Music, Snapdragon	https://www. qualcomm.co m/company/ product- security/bull etins/august- 2021-bulletin	0-QUA-SD67- 200921/3284

 CVSS Scoring Scale
 0-1
 1-2
 2-3
 3-4
 4-5

5-6

6-7

7-8

8-9

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Wearables		
			CVE ID : CVE-2021-1914		
Out-of- bounds Write	08-Sep-21	10	Possible buffer underflow due to lack of check for negative indices values when processing user provided input in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Voice & Music, Snapdragon Wearables	https://www. qualcomm.co m/company/ product- security/bull etins/august- 2021-bulletin	0-QUA-SD67- 200921/3285
			CVE ID : CVE-2021-1916		
Integer Underflow (Wrap or Wraparoun d)	08-Sep-21	10	Integer underflow can occur when the RTCP length is lesser than than the actual blocks present in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Voice & Music, Snapdragon Wearables CVE ID : CVE-2021-1919	https://www. qualcomm.co m/company/ product- security/bull etins/august- 2021-bulletin	0-QUA-SD67- 200921/3286
Integer Underflow (Wrap or Wraparoun d)	08-Sep-21	10	Integer underflow can occur due to improper handling of incoming RTCP packets in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Voice & Music, Snapdragon Wearables	https://www. qualcomm.co m/company/ product- security/bull etins/august- 2021-bulletin	0-QUA-SD67- 200921/3287
CVSS Scoring Sc	ale 0-1	1-2	2-3 3-4 4-5 5-6	6-7 7-8	8-9 9-10

Page 1269 of 1474

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2021-1920		
Incorrect Type Conversion or Cast	08-Sep-21	4.6	Incorrect pointer argument passed to trusted application TA could result in un- intended memory operations in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Industrial IOT CVE ID : CVE-2021-1923	https://www. qualcomm.co m/company/ product- security/bull etins/august- 2021-bulletin	0-QUA-SD67- 200921/3288
Exposure of Resource to Wrong Sphere	08-Sep-21	2.1	Lack of strict validation of bootmode can lead to information disclosure in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wearables CVE ID : CVE-2021-1929	https://www. qualcomm.co m/company/ product- security/bull etins/august- 2021-bulletin	0-QUA-SD67- 200921/3289
Improper Restriction of Operations within the Bounds of a Memory Buffer	08-Sep-21	3.6	Possible out of bounds read due to incorrect validation of incoming buffer length in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile CVE ID : CVE-2021-1930	https://www. qualcomm.co m/company/ product- security/bull etins/august- 2021-bulletin	0-QUA-SD67- 200921/3290
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	08-Sep-21	10	Possible buffer overflow due to improper validation of device types during P2P search in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT,	https://www. qualcomm.co m/company/ product- security/bull etins/august- 2021-bulletin	0-QUA-SD67- 200921/3291

Page 1270 of 1474

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking		
			CVE ID : CVE-2021-1972		
sd690_5g_fir	mware			Γ	I
Exposure of Resource to Wrong Sphere	08-Sep-21	2.1	Child process can leak information from parent process due to numeric pids are getting compared and these pid can be reused in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wearables CVE ID : CVE-2021-1904	https://www. qualcomm.co m/company/ product- security/bull etins/august- 2021-bulletin	0-QUA-SD69- 200921/3292
Loop with Unreachable Exit Condition ('Infinite Loop')	08-Sep-21	5	Loop with unreachable exit condition may occur due to improper handling of unsupported input in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Voice & Music, Snapdragon Wearables CVE ID : CVE-2021-1914	https://www. qualcomm.co m/company/ product- security/bull etins/august- 2021-bulletin	0-QUA-SD69- 200921/3293
Out-of- bounds	08-Sep-21	10	Possible buffer underflow due to lack of check for	https://www. qualcomm.co	0-QUA-SD69- 200921/3294
CVSS Scoring Sco	ale 0-1	1-2	aue to lack of check for 2-3 3-4 4-5 5-6 Page 1271 of 1474	qualcomm.co	8-9 9-10

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Write			negative indices values when processing user provided input in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Voice & Music, Snapdragon Wearables CVE ID : CVE-2021-1916	m/company/ product- security/bull etins/august- 2021-bulletin	
Integer Underflow (Wrap or Wraparoun d)	08-Sep-21	10	Integer underflow can occur when the RTCP length is lesser than than the actual blocks present in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Voice & Music, Snapdragon Wearables CVE ID : CVE-2021-1919	https://www. qualcomm.co m/company/ product- security/bull etins/august- 2021-bulletin	0-QUA-SD69- 200921/3295
Integer Underflow (Wrap or Wraparoun d)	08-Sep-21	10	Integer underflow can occur due to improper handling of incoming RTCP packets in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Voice & Music, Snapdragon Wearables	https://www. qualcomm.co m/company/ product- security/bull etins/august- 2021-bulletin	0-QUA-SD69- 200921/3296
Incorrect	09 San 21	1.6	CVE ID : CVE-2021-1920 Incorrect pointer argument	https://www.	0-QUA-SD69-
Type Conversion	08-Sep-21	4.6	passed to trusted application TA could result in un-	qualcomm.co m/company/	200921/3297

CVSS Scoring Scale	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10		
	Page 1272 of 1474											

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
or Cast			intended memory operations in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Industrial IOT	product- security/bull etins/august- 2021-bulletin	
			CVE ID : CVE-2021-1923		
Improper Restriction of Operations within the Bounds of a Memory Buffer	08-Sep-21	3.6	Possible out of bounds read due to incorrect validation of incoming buffer length in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile	https://www. qualcomm.co m/company/ product- security/bull etins/august- 2021-bulletin	0-QUA-SD69- 200921/3298
			CVE ID : CVE-2021-1930		
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	08-Sep-21	10	Possible buffer overflow due to improper validation of device types during P2P search in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Woice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking CVE ID : CVE-2021-1972	https://www. qualcomm.co m/company/ product- security/bull etins/august- 2021-bulletin	0-QUA-SD69- 200921/3299
sd710_firmw	are				
Exposure of Resource to Wrong Sphere	08-Sep-21	2.1	Child process can leak information from parent process due to numeric pids are getting compared and these pid can be reused in Snapdragon Auto,	https://www. qualcomm.co m/company/ product- security/bull etins/august-	0-QUA-SD71- 200921/3300
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 & CVE ID	Patch	NCIIPC ID							
			Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables CVE ID : CVE-2021-1904	2021-bulletin								
Improper Restriction of Operations within the Bounds of a Memory Buffer	08-Sep-21	3.6	Possible out of bounds read due to incorrect validation of incoming buffer length in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile	https://www. qualcomm.co m/company/ product- security/bull etins/august- 2021-bulletin	0-QUA-SD71- 200921/3301							
			CVE ID : CVE-2021-1930 Possible buffer overflow due									
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	08-Sep-21	10	to improper validation of device types during P2P search in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Woice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking CVE ID : CVE-2021-1972	https://www. qualcomm.co m/company/ product- security/bull etins/august- 2021-bulletin	0-QUA-SD71- 200921/3302							
sd712_firmw	are											
Loop with Unreachable Exit Condition	08-Sep-21	5	Loop with unreachable exit condition may occur due to improper handling of unsupported input in	https://www. qualcomm.co m/company/ product-	0-QUA-SD71- 200921/3303							
CVSS Scoring Sca	ale 0-1	1-2	2-3 3-4 4-5 5-6	6-7 7-8								

Page 1274 of 1474

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
('Infinite Loop')			Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Voice & Music, Snapdragon Wearables	security/bull etins/august- 2021-bulletin	
Out-of- bounds Write	08-Sep-21	10	CVE ID : CVE-2021-1914 Possible buffer underflow due to lack of check for negative indices values when processing user provided input in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Voice & Music, Snapdragon Wearables CVE ID : CVE-2021-1916	https://www. qualcomm.co m/company/ product- security/bull etins/august- 2021-bulletin	O-QUA-SD71- 200921/3304
Integer Underflow (Wrap or Wraparoun d)	08-Sep-21	10	Integer underflow can occur when the RTCP length is lesser than than the actual blocks present in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Voice & Music, Snapdragon Wearables CVE ID : CVE-2021-1919	https://www. qualcomm.co m/company/ product- security/bull etins/august- 2021-bulletin	0-QUA-SD71- 200921/3305
Integer Underflow (Wrap or Wraparoun	08-Sep-21	10	Integer underflow can occur due to improper handling of incoming RTCP packets in Snapdragon Auto,	https://www. qualcomm.co m/company/ product-	O-QUA-SD71- 200921/3306

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
d)			Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Voice & Music, Snapdragon Wearables CVE ID : CVE-2021-1920	security/bull etins/august- 2021-bulletin	
sd720g_firm	ware				
Exposure of Resource to Wrong Sphere	08-Sep-21	2.1	Child process can leak information from parent process due to numeric pids are getting compared and these pid can be reused in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wearables CVE ID : CVE-2021-1904	https://www. qualcomm.co m/company/ product- security/bull etins/august- 2021-bulletin	0-QUA-SD72- 200921/3307
Loop with Unreachable Exit Condition ('Infinite Loop')	08-Sep-21	5	Loop with unreachable exit condition may occur due to improper handling of unsupported input in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Voice & Music, Snapdragon Wearables CVE ID : CVE-2021-1914	https://www. qualcomm.co m/company/ product- security/bull etins/august- 2021-bulletin	0-QUA-SD72- 200921/3308
Out-of- bounds	08-Sep-21	10	Possible buffer underflow due to lack of check for	https://www. qualcomm.co	0-QUA-SD72- 200921/3309

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Write			negative indices values when processing user provided input in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Voice & Music, Snapdragon Wearables CVE ID : CVE-2021-1916	m/company/ product- security/bull etins/august- 2021-bulletin	
Integer Underflow (Wrap or Wraparoun d)	08-Sep-21	10	Integer underflow can occur when the RTCP length is lesser than than the actual blocks present in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Voice & Music, Snapdragon Wearables CVE ID : CVE-2021-1919	https://www. qualcomm.co m/company/ product- security/bull etins/august- 2021-bulletin	0-QUA-SD72- 200921/3310
Integer Underflow (Wrap or Wraparoun d)	08-Sep-21	10	Integer underflow can occur due to improper handling of incoming RTCP packets in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Voice & Music, Snapdragon Wearables	https://www. qualcomm.co m/company/ product- security/bull etins/august- 2021-bulletin	0-QUA-SD72- 200921/3311
Incorrect	08-Sep-21	4.6	CVE ID : CVE-2021-1920 Incorrect pointer argument	https://www.	O-QUA-SD72-
Type Conversion	00 369-21	1.0	passed to trusted application TA could result in un-	qualcomm.co m/company/	200921/3312

CVSS Scoring Scale	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10	
Page 1277 of 1474											

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
or Cast			intended memory operations in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Industrial IOT CVE ID : CVE-2021-1923	product- security/bull etins/august- 2021-bulletin	
Exposure of Resource to Wrong Sphere	08-Sep-21	2.1	Lack of strict validation of bootmode can lead to information disclosure in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wearables CVE ID : CVE-2021-1929	https://www. qualcomm.co m/company/ product- security/bull etins/august- 2021-bulletin	0-QUA-SD72- 200921/3313
Improper Restriction of Operations within the Bounds of a Memory Buffer	08-Sep-21	3.6	Possible out of bounds read due to incorrect validation of incoming buffer length in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile CVE ID : CVE-2021-1930	https://www. qualcomm.co m/company/ product- security/bull etins/august- 2021-bulletin	O-QUA-SD72- 200921/3314
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	08-Sep-21	10	Possible buffer overflow due to improper validation of device types during P2P search in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables,	https://www. qualcomm.co m/company/ product- security/bull etins/august- 2021-bulletin	0-QUA-SD72- 200921/3315

0-1

1-2 2-3 3-4

Page 1278 of 1474

4-5

5-6

6-7

7-8

8-9

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Snapdragon Wired Infrastructure and Networking		
			CVE ID : CVE-2021-1972		
sd730_firmw	are				
Exposure of Resource to Wrong Sphere	08-Sep-21	2.1	Child process can leak information from parent process due to numeric pids are getting compared and these pid can be reused in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wearables CVE ID : CVE-2021-1904	https://www. qualcomm.co m/company/ product- security/bull etins/august- 2021-bulletin	O-QUA-SD73- 200921/3316
Loop with Unreachable Exit Condition ('Infinite Loop')	08-Sep-21	5	Loop with unreachable exit condition may occur due to improper handling of unsupported input in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Voice & Music, Snapdragon Wearables CVE ID : CVE-2021-1914	https://www. qualcomm.co m/company/ product- security/bull etins/august- 2021-bulletin	0-QUA-SD73- 200921/3317
Out-of- bounds Write	08-Sep-21	10	Possible buffer underflow due to lack of check for negative indices values when processing user provided input in Snapdragon Auto, Snapdragon Compute,	https://www. qualcomm.co m/company/ product- security/bull etins/august-	0-QUA-SD73- 200921/3318
CVSS Scoring Sc	ale 0-1	1-2	2-3 3-4 4-5 5-6	6-7 7-8	8-9 9-10

Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
		Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Voice & Music, Snapdragon Wearables	2021-bulletin	
		CVE ID : CVE-2021-1916		
08-Sep-21	10	Integer underflow can occur when the RTCP length is lesser than than the actual blocks present in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Voice & Music, Snapdragon Wearables	https://www. qualcomm.co m/company/ product- security/bull etins/august- 2021-bulletin	0-QUA-SD73- 200921/3319
		CVE ID : CVE-2021-1919		
08-Sep-21	10	Integer underflow can occur due to improper handling of incoming RTCP packets in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Voice & Music, Snapdragon Wearables CVE ID : CVE-2021-1920	https://www. qualcomm.co m/company/ product- security/bull etins/august- 2021-bulletin	0-QUA-SD73- 200921/3320
08-Sep-21	4.6	Incorrect pointer argument passed to trusted application TA could result in un- intended memory operations in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity,	https://www. qualcomm.co m/company/ product- security/bull etins/august- 2021-bulletin	0-QUA-SD73- 200921/3321
	08-Sep-21	08-Sep-21 10 08-Sep-21 10	08-Sep-21Integer underflow can occur when the RTCP length is lesser than than the actual blocks present in Snapdragon Voice & Music, Snapdragon Wearables08-Sep-211010Integer underflow can occur when the RTCP length is lesser than than the actual blocks present in Snapdragon Auto, Snapdragon Compute, Snapdragon IoT, Snapdragon Voice & Music, Snapdragon Owice & Music, Snapdragon Outice & Music, Snapdragon Core & Music, Snapdragon Voice & Music, Snapdragon Snapdragon Compute, Snapdragon Industrial IOT, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Indu	08-Sep-21110Snapdragon Connectivity, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Voice & Music, Snapdragon Wearables2021-bulletin08-Sep-21110Integer underflow can occur when the RTCP length is lesser than than the actual blocks present in Snapdragon Auto, Snapdragon Consumer IOT, Snapdragon Consumer IOT, Snapdragon Consumer IOT, Snapdragon IoU, Snapdragon Music, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoU, Snapdragon Voice & Music, Snapdragon Voice & Music

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Snapdragon Industrial IOT		
			CVE ID : CVE-2021-1923		
Exposure of Resource to Wrong Sphere	08-Sep-21	2.1	Lack of strict validation of bootmode can lead to information disclosure in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wearables CVE ID : CVE-2021-1929	https://www. qualcomm.co m/company/ product- security/bull etins/august- 2021-bulletin	0-QUA-SD73- 200921/3322
Improper Restriction of Operations within the Bounds of a Memory Buffer	08-Sep-21	3.6	Possible out of bounds read due to incorrect validation of incoming buffer length in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile CVE ID : CVE-2021-1930	https://www. qualcomm.co m/company/ product- security/bull etins/august- 2021-bulletin	0-QUA-SD73- 200921/3323
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	08-Sep-21	10	Possible buffer overflow due to improper validation of device types during P2P search in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Woice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking CVE ID : CVE-2021-1972	https://www. qualcomm.co m/company/ product- security/bull etins/august- 2021-bulletin	0-QUA-SD73- 200921/3324
CVSS Scoring Sc	ale 0-1	1-2	2-3 3-4 4-5 5-6	6-7 7-8	8-9 9-10

Page 1281 of 1474

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
sd750g_firm					
Exposure of Resource to Wrong Sphere	08-Sep-21	2.1	Child process can leak information from parent process due to numeric pids are getting compared and these pid can be reused in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wearables CVE ID : CVE-2021-1904	https://www. qualcomm.co m/company/ product- security/bull etins/august- 2021-bulletin	0-QUA-SD75- 200921/3325
Loop with Unreachable Exit Condition ('Infinite Loop')	08-Sep-21	5	Loop with unreachable exit condition may occur due to improper handling of unsupported input in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Voice & Music, Snapdragon Wearables CVE ID : CVE-2021-1914	https://www. qualcomm.co m/company/ product- security/bull etins/august- 2021-bulletin	0-QUA-SD75- 200921/3326
Out-of- bounds 08-Sep-21 Write 08-Sep-21		10	Possible buffer underflow due to lack of check for negative indices values when processing user provided input in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Voice & Music, Snapdragon	https://www. qualcomm.co m/company/ product- security/bull etins/august- 2021-bulletin	0-QUA-SD75- 200921/3327

Page 1282 of 1474

Weakness	· · ·		Patch	NCIIPC ID	
			Wearables		
			CVE ID : CVE-2021-1916		
Integer Underflow (Wrap or Wraparoun d)	08-Sep-21	10	Integer underflow can occur when the RTCP length is lesser than than the actual blocks present in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Voice & Music, Snapdragon Wearables	https://www. qualcomm.co m/company/ product- security/bull etins/august- 2021-bulletin	0-QUA-SD75- 200921/3328
			CVE ID : CVE-2021-1919		
Integer Underflow (Wrap or Wraparoun d)	08-Sep-21	10	Integer underflow can occur due to improper handling of incoming RTCP packets in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Voice & Music, Snapdragon Wearables CVE ID : CVE-2021-1920	https://www. qualcomm.co m/company/ product- security/bull etins/august- 2021-bulletin	0-QUA-SD75- 200921/3329
Incorrect Type Conversion or Cast	08-Sep-21	-21Incorrect pointer argument passed to trusted application TA could result in un- intended memory operations in Snapdragon Auto, Snapdragon Compute, Snapdragon Industrial IOThttps://www. qualcomm.co m/company/ product- security/bull etins/august- 2021-bulletin		0-QUA-SD75- 200921/3330	
Improper Restriction of	08-Sep-21	3.6	Possible out of bounds read due to incorrect validation of incoming buffer length in	https://www. qualcomm.co m/company/	0-QUA-SD75- 200921/3331
CVSS Scoring Sc	ale 0-1	1-2	2-3 3-4 4-5 5-6	6-7 7-8	8-9 <u>9-10</u>

		CVSS	Description & CVE ID	Patch	NCIIPC ID
Operations within the Bounds of a Memory Buffer			Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile	product- security/bull etins/august- 2021-bulletin	
			CVE ID : CVE-2021-1930		
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	08-Sep-21	10	Possible buffer overflow due to improper validation of device types during P2P search in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Industrial IOT, Snapdragon Woile, Snapdragon Woice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking CVE ID : CVE-2021-1972	https://www. qualcomm.co m/company/ product- security/bull etins/august- 2021-bulletin	0-QUA-SD75- 200921/3332
sd765g_firmw	/are				L
Exposure of Resource to		2.1	Child process can leak information from parent process due to numeric pids are getting compared and these pid can be reused in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wearables CVE ID : CVE-2021-1904	https://www. qualcomm.co m/company/ product- security/bull etins/august- 2021-bulletin	0-QUA-SD76- 200921/3333

Page 1284 of 1474

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Unreachable Exit Condition ('Infinite Loop')			condition may occur due to improper handling of unsupported input in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Voice & Music, Snapdragon Wearables CVE ID : CVE-2021-1914	qualcomm.co m/company/ product- security/bull etins/august- 2021-bulletin	200921/3334
Out-of- bounds Write	08-Sep-21	10	Possible buffer underflow due to lack of check for negative indices values when processing user provided input in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Voice & Music, Snapdragon Wearables	https://www. qualcomm.co m/company/ product- security/bull etins/august- 2021-bulletin	0-QUA-SD76- 200921/3335
Integer Underflow (Wrap or Wraparoun d)	08-Sep-21	10	CVE ID : CVE-2021-1916 Integer underflow can occur when the RTCP length is lesser than than the actual blocks present in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Voice & Music, Snapdragon Wearables CVE ID : CVE-2021-1919	https://www. qualcomm.co m/company/ product- security/bull etins/august- 2021-bulletin	0-QUA-SD76- 200921/3336
	08-Sep-21	10	Integer underflow can occur	https://www.	0-QUA-SD76-

Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
		due to improper handling of incoming RTCP packets in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Voice & Music, Snapdragon Wearables CVE ID : CVE-2021-1920	qualcomm.co m/company/ product- security/bull etins/august- 2021-bulletin	200921/3337
08-Sep-21	4.6	Incorrect pointer argument passed to trusted application TA could result in un- intended memory operations in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Industrial IOT CVE ID : CVE-2021-1923	https://www. qualcomm.co m/company/ product- security/bull etins/august- 2021-bulletin	0-QUA-SD76- 200921/3338
08-Sep-21	2.1	Lack of strict validation of bootmode can lead to information disclosure in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wearables CVE ID : CVE-2021-1929	https://www. qualcomm.co m/company/ product- security/bull etins/august- 2021-bulletin	0-QUA-SD76- 200921/3339
08-Sep-21	3.6	Possible out of bounds read due to incorrect validation of incoming buffer length in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT,	https://www. qualcomm.co m/company/ product- security/bull etins/august- 2021-bulletin	O-QUA-SD76- 200921/3340
	08-Sep-21	08-Sep-21 4.6 08-Sep-21 2.1	Image: construct of the second seco	08-Sep-2110due to improper handling of incoming RTCP packets in Snapdragon Compute, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Compute, Snapdragon Compute, Snapdragon Industrial IOThttps://www. qualcomm.co m/company/ product- security/bull etins/august- 2021-bulletin08-Sep-2114.66Lack of strict validation of bootmode can lead to information disclosure in Snapdragon Compute, Snapdragon Compute, Snapdragon Compute, Snapdragon Industrial IOT, Snapdragon Consumer IOT, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Mobile, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Mobile, Snapdragon Mobile, Snapdragon Industrial IOT, Snapdragon Industrial IOT, Snapdragon Industrial IOT, Snapdragon Industrial IOT, Snapdragon Industrial IOT, Snapdragon

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Buffer			Snapdragon Industrial IOT, Snapdragon Mobile		
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	08-Sep-21	Sep-2110CVE ID : CVE-2021-1930Sep-2110Possible buffer overflow due to improper validation of device types during P2P search in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wearables, Snapdragon Wired Infrastructure and NetworkingCVE ID : CVE-2021-1972		https://www. qualcomm.co m/company/ product- security/bull etins/august- 2021-bulletin	0-QUA-SD76- 200921/3341
sd765_firmw	are				
Exposure of Resource to Wrong Sphere	08-Sep-21	2.1	Child process can leak information from parent process due to numeric pids are getting compared and these pid can be reused in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wearables CVE ID : CVE-2021-1904	https://www. qualcomm.co m/company/ product- security/bull etins/august- 2021-bulletin	0-QUA-SD76- 200921/3342
Loop with Unreachable Exit Condition ('Infinite	08-Sep-21	5	Loop with unreachable exit condition may occur due to improper handling of unsupported input in Snapdragon Auto,	https://www. qualcomm.co m/company/ product- security/bull	0-QUA-SD76- 200921/3343
CVSS Scoring Sc	ale 0-1	1-2	2-3 3-4 4-5 5-6	6-7 7-8	8-9 9-10

Page 1287 of 1474

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Loop')			Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Voice & Music, Snapdragon Wearables CVE ID : CVE-2021-1914	etins/august- 2021-bulletin	
Out-of- bounds Write	08-Sep-21	10	Possible buffer underflow due to lack of check for negative indices values when processing user provided input in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Voice & Music, Snapdragon Wearables CVE ID : CVE-2021-1916	https://www. qualcomm.co m/company/ product- security/bull etins/august- 2021-bulletin	0-QUA-SD76- 200921/3344
Integer Underflow (Wrap or Wraparoun d)	08-Sep-21	10	Integer underflow can occur when the RTCP length is lesser than than the actual blocks present in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity,		0-QUA-SD76- 200921/3345
Integer Underflow (Wrap or Wraparoun d)	08-Sep-21	10	Integer underflow can occur due to improper handling of incoming RTCP packets in Snapdragon Auto, Snapdragon Compute,	https://www. qualcomm.co m/company/ product- security/bull	0-QUA-SD76- 200921/3346
CVSS Scoring Sc	ale 0-1	1-2	2-3 3-4 4-5 5-6	6-7 7-8	8-9 9-10

 3-4
 4-5
 5-6
 6-7

 Page 1288 of 1474

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Voice & Music, Snapdragon Wearables	etins/august- 2021-bulletin	
			CVE ID : CVE-2021-1920		
Incorrect Type Conversion or Cast	08-Sep-21	4.6	Incorrect pointer argument passed to trusted application TA could result in un- intended memory operations in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Industrial IOT CVE ID : CVE-2021-1923	https://www. qualcomm.co m/company/ product- security/bull etins/august- 2021-bulletin	0-QUA-SD76- 200921/3347
Exposure of Resource to Wrong Sphere	08-Sep-21	2.1	Lack of strict validation of bootmode can lead to information disclosure in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wearables CVE ID : CVE-2021-1929	https://www. qualcomm.co m/company/ product- security/bull etins/august- 2021-bulletin	O-QUA-SD76- 200921/3348
Improper Restriction of Operations within the Bounds of a Memory Buffer	08-Sep-21	3.6	Possible out of bounds read due to incorrect validation of incoming buffer length in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile CVE ID : CVE-2021-1930	https://www. qualcomm.co m/company/ product- security/bull etins/august- 2021-bulletin	O-QUA-SD76- 200921/3349

CVSS Scoring Scale	0-1	1-2	2-3	3-4	4-5	5-6
			De	a 1200	of 1 1 7 1	

7-8

6-7

8-9

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	08-Sep-21	10	Possible buffer overflow due to improper validation of device types during P2P search in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Woice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking CVE ID : CVE-2021-1972	https://www. qualcomm.co m/company/ product- security/bull etins/august- 2021-bulletin	0-QUA-SD76- 200921/3350
sd768g_firm	ware				
Exposure of Resource to Wrong Sphere			Child process can leak information from parent process due to numeric pids are getting compared and these pid can be reused in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables CVE ID : CVE-2021-1904	https://www. qualcomm.co m/company/ product- security/bull etins/august- 2021-bulletin	0-QUA-SD76- 200921/3351
Loop with Unreachable Exit Condition ('Infinite Loop')	08-Sep-21	5	Loop with unreachable exit condition may occur due to improper handling of unsupported input in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT,	https://www. qualcomm.co m/company/ product- security/bull etins/august- 2021-bulletin	0-QUA-SD76- 200921/3352

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Snapdragon IoT, Snapdragon Voice & Music, Snapdragon Wearables		
			CVE ID : CVE-2021-1914		
Out-of- bounds Write	08-Sep-21	10	Possible buffer underflow due to lack of check for negative indices values when processing user provided input in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Voice & Music, Snapdragon Wearables	https://www. qualcomm.co m/company/ product- security/bull etins/august- 2021-bulletin	O-QUA-SD76- 200921/3353
			CVE ID : CVE-2021-1916		
Integer Underflow (Wrap or Wraparoun d)	08-Sep-21	10	Integer underflow can occur when the RTCP length is lesser than than the actual blocks present in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Voice & Music, Snapdragon Wearables	https://www. qualcomm.co m/company/ product- security/bull etins/august- 2021-bulletin	O-QUA-SD76- 200921/3354
			CVE ID : CVE-2021-1919		
Integer Underflow (Wrap or Wraparoun d)	08-Sep-21	10	Integer underflow can occur due to improper handling of incoming RTCP packets in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon	https://www. qualcomm.co m/company/ product- security/bull etins/august- 2021-bulletin	0-QUA-SD76- 200921/3355

0-1

1-2

2-3 3-4

4-5

5-6

6-7

7-8

8-9

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Voice & Music, Snapdragon Wearables		
			CVE ID : CVE-2021-1920		
Incorrect Type Conversion or Cast	08-Sep-21	4.6	Incorrect pointer argument passed to trusted application TA could result in un- intended memory operations in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Industrial IOT CVE ID : CVE-2021-1923	https://www. qualcomm.co m/company/ product- security/bull etins/august- 2021-bulletin	0-QUA-SD76- 200921/3356
Exposure of Resource to Wrong Sphere	08-Sep-21	2.1	Lack of strict validation of bootmode can lead to information disclosure in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wearables CVE ID : CVE-2021-1929	https://www. qualcomm.co m/company/ product- security/bull etins/august- 2021-bulletin	0-QUA-SD76- 200921/3357
Improper Restriction of Operations within the Bounds of a Memory Buffer	08-Sep-21	3.6	Possible out of bounds read due to incorrect validation of incoming buffer length in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile CVE ID : CVE-2021-1930	https://www. qualcomm.co m/company/ product- security/bull etins/august- 2021-bulletin	0-QUA-SD76- 200921/3358
Buffer Copy without Checking Size of Input ('Classic	08-Sep-21	10	Possible buffer overflow due to improper validation of device types during P2P search in Snapdragon Auto, Snapdragon Compute,	https://www. qualcomm.co m/company/ product- security/bull	0-QUA-SD76- 200921/3359

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Buffer Overflow')			Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking CVE ID : CVE-2021-1972	etins/august- 2021-bulletin	
sd778g_firm	ware			L	
Exposure of Resource to Wrong Sphere	08-Sep-21	2.1	Child process can leak information from parent process due to numeric pids are getting compared and these pid can be reused in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wearables CVE ID : CVE-2021-1904	https://www. qualcomm.co m/company/ product- security/bull etins/august- 2021-bulletin	O-QUA-SD77- 200921/3360
Loop with Unreachable Exit Condition ('Infinite Loop')	08-Sep-21	5	Loop with unreachable exit condition may occur due to improper handling of unsupported input in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Voice & Music, Snapdragon Wearables CVE ID : CVE-2021-1914	https://www. qualcomm.co m/company/ product- security/bull etins/august- 2021-bulletin	0-QUA-SD77- 200921/3361
CVSS Scoring Scale 0-1 1-2 2-3 3-4 4-5 5-6 6-7 7-8 8-9 9-10					

 3-4
 4-5
 5-6

 Page 1293 of 1474

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Out-of- bounds Write	08-Sep-21	10	Possible buffer underflow due to lack of check for negative indices values when processing user provided input in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Voice & Music, Snapdragon Wearables	https://www. qualcomm.co m/company/ product- security/bull etins/august- 2021-bulletin	0-QUA-SD77- 200921/3362
			CVE ID : CVE-2021-1916 Integer underflow can occur		
Integer Underflow (Wrap or Wraparoun d)	08-Sep-21	10	when the RTCP length is lesser than than the actual blocks present in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Voice & Music, Snapdragon Wearables	https://www. qualcomm.co m/company/ product- security/bull etins/august- 2021-bulletin	0-QUA-SD77- 200921/3363
			CVE ID : CVE-2021-1919		
Integer Underflow (Wrap or Wraparoun d)	08-Sep-21	10	Integer underflow can occur due to improper handling of incoming RTCP packets in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Voice & Music, Snapdragon Wearables CVE ID : CVE-2021-1920	https://www. qualcomm.co m/company/ product- security/bull etins/august- 2021-bulletin	0-QUA-SD77- 200921/3364

 3-4
 4-5
 5-6

 Page 1294 of 1474

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Type Conversion or Cast			passed to trusted application TA could result in un- intended memory operations in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Industrial IOT CVE ID : CVE-2021-1923	qualcomm.co m/company/ product- security/bull etins/august- 2021-bulletin	200921/3365
Exposure of Resource to Wrong Sphere	08-Sep-21	2.1	Lack of strict validation of bootmode can lead to information disclosure in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wearables CVE ID : CVE-2021-1929	https://www. qualcomm.co m/company/ product- security/bull etins/august- 2021-bulletin	0-QUA-SD77- 200921/3366
Improper Restriction of Operations within the Bounds of a Memory Buffer	08-Sep-21	3.6	Possible out of bounds read due to incorrect validation of incoming buffer length in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile CVE ID : CVE-2021-1930	https://www. qualcomm.co m/company/ product- security/bull etins/august- 2021-bulletin	0-QUA-SD77- 200921/3367
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	08-Sep-21	10	Possible buffer overflow due to improper validation of device types during P2P search in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile,	https://www. qualcomm.co m/company/ product- security/bull etins/august- 2021-bulletin	0-QUA-SD77- 200921/3368

0-1

1-2

4-5

5-6

6-7

7-8

8-9

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID			
			Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking					
			CVE ID : CVE-2021-1972					
sd780g_firmv	sd780g_firmware							
Exposure of Resource to Wrong Sphere	08-Sep-21	2.1	Child process can leak information from parent process due to numeric pids are getting compared and these pid can be reused in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wearables CVE ID : CVE-2021-1904	https://www. qualcomm.co m/company/ product- security/bull etins/august- 2021-bulletin	0-QUA-SD78- 200921/3369			
Out-of- bounds Write	08-Sep-21	10	Possible buffer underflow due to lack of check for negative indices values when processing user provided input in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Voice & Music, Snapdragon Wearables CVE ID : CVE-2021-1916	https://www. qualcomm.co m/company/ product- security/bull etins/august- 2021-bulletin	0-QUA-SD78- 200921/3370			
Incorrect Type Conversion or Cast	08-Sep-21	4.6	Incorrect pointer argument passed to trusted application TA could result in un- intended memory operations	https://www. qualcomm.co m/company/ product-	0-QUA-SD78- 200921/3371			
CVSS Scoring Scale 0-1 1-2 2-3 3-4 4-5 5-6 6-7 7-8 8-9 9-10								

Page 1296 of 1474

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Industrial IOT CVE ID : CVE-2021-1923	security/bull etins/august- 2021-bulletin	
Exposure of Resource to Wrong Sphere	08-Sep-21	2.1	Lack of strict validation of bootmode can lead to information disclosure in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wearables CVE ID : CVE-2021-1929	https://www. qualcomm.co m/company/ product- security/bull etins/august- 2021-bulletin	O-QUA-SD78- 200921/3372
Improper Restriction of Operations within the Bounds of a Memory Buffer	08-Sep-21	3.6	Possible out of bounds read due to incorrect validation of incoming buffer length in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile CVE ID : CVE-2021-1930	https://www. qualcomm.co m/company/ product- security/bull etins/august- 2021-bulletin	O-QUA-SD78- 200921/3373
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	08-Sep-21	10	Possible buffer overflow due to improper validation of device types during P2P search in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Woice & Music, Snapdragon Wearables, Snapdragon Wired	https://www. qualcomm.co m/company/ product- security/bull etins/august- 2021-bulletin	0-QUA-SD78- 200921/3374

0-1

1-2

7-8

5-6

6-7

8-9

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Infrastructure and Networking		
			CVE ID : CVE-2021-1972		
sd7c_firmwa	re			1	1
Improper Restriction of Operations within the Bounds of a Memory Buffer	08-Sep-21	3.6	Possible out of bounds read due to incorrect validation of incoming buffer length in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile	https://www. qualcomm.co m/company/ product- security/bull etins/august- 2021-bulletin	0-QUA-SD7C- 200921/3375
			CVE ID : CVE-2021-1930		
sd820_firmw	vare			I	I
Loop with Unreachable Exit Condition ('Infinite Loop')	08-Sep-21	5	Loop with unreachable exit condition may occur due to improper handling of unsupported input in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Voice & Music, Snapdragon Wearables CVE ID : CVE-2021-1914	https://www. qualcomm.co m/company/ product- security/bull etins/august- 2021-bulletin	0-QUA-SD82- 200921/3376
Out-of- bounds Write	08-Sep-21	10	Possible buffer underflow due to lack of check for negative indices values when processing user provided input in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon	https://www. qualcomm.co m/company/ product- security/bull etins/august- 2021-bulletin	0-QUA-SD82- 200921/3377

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Voice & Music, Snapdragon Wearables CVE ID : CVE-2021-1916		
Integer Underflow (Wrap or Wraparoun d)	08-Sep-21	10	Integer underflow can occur when the RTCP length is lesser than than the actual blocks present in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Voice & Music, Snapdragon Wearables	https://www. qualcomm.co m/company/ product- security/bull etins/august- 2021-bulletin	O-QUA-SD82- 200921/3378
			CVE ID : CVE-2021-1919		
Integer Underflow (Wrap or Wraparoun d)	08-Sep-21	10	Integer underflow can occur due to improper handling of incoming RTCP packets in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Voice & Music, Snapdragon Wearables CVE ID : CVE-2021-1920	https://www. qualcomm.co m/company/ product- security/bull etins/august- 2021-bulletin	0-QUA-SD82- 200921/3379
sd821_firmw	are				
Loop with Unreachable Exit Condition ('Infinite Loop')	08-Sep-21	5	Loop with unreachable exit condition may occur due to improper handling of unsupported input in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon	https://www. qualcomm.co m/company/ product- security/bull etins/august- 2021-bulletin	O-QUA-SD82- 200921/3380
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 & CVE ID	Patch	NCIIPC ID
			Voice & Music, Snapdragon Wearables		
			CVE ID : CVE-2021-1914		
Out-of- bounds Write	08-Sep-21	10	Possible buffer underflow due to lack of check for negative indices values when processing user provided input in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Voice & Music, Snapdragon Wearables CVE ID : CVE-2021-1916	https://www. qualcomm.co m/company/ product- security/bull etins/august- 2021-bulletin	O-QUA-SD82- 200921/3381
Integer Underflow (Wrap or Wraparoun d)	08-Sep-21	10	Integer underflow can occur when the RTCP length is lesser than than the actual blocks present in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Voice & Music, Snapdragon Wearables	https://www. qualcomm.co m/company/ product- security/bull etins/august- 2021-bulletin	0-QUA-SD82- 200921/3382
			CVE ID : CVE-2021-1919		
Integer Underflow (Wrap or Wraparoun d)	08-Sep-21	10	Integer underflow can occur due to improper handling of incoming RTCP packets in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Voice & Music, Snapdragon	https://www. qualcomm.co m/company/ product- security/bull etins/august- 2021-bulletin	O-QUA-SD82- 200921/3383

1-2

0-1

5-6

6-7

7-8

8-9

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Wearables		
			CVE ID : CVE-2021-1920		
sd835_firmw	are				
Exposure of Resource to Wrong Sphere	08-Sep-21	2.1	Child process can leak information from parent process due to numeric pids are getting compared and these pid can be reused in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wearables CVE ID : CVE-2021-1904	https://www. qualcomm.co m/company/ product- security/bull etins/august- 2021-bulletin	0-QUA-SD83- 200921/3384
Loop with Unreachable Exit Condition ('Infinite Loop')	08-Sep-21	5	Loop with unreachable exit condition may occur due to improper handling of unsupported input in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Voice & Music, Snapdragon Wearables CVE ID : CVE-2021-1914	https://www. qualcomm.co m/company/ product- security/bull etins/august- 2021-bulletin	0-QUA-SD83- 200921/3385
Out-of- bounds Write	08-Sep-21	10	Possible buffer underflow due to lack of check for negative indices values when processing user provided input in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT,	https://www. qualcomm.co m/company/ product- security/bull etins/august- 2021-bulletin	0-QUA-SD83- 200921/3386
CVSS Scoring Sc	ale 0-1	1-2	2-3 3-4 4-5 5-6	6-7 7-8	8-9 9-10

Page 1301 of 1474

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Voice & Music, Snapdragon Wearables CVE ID : CVE-2021-1916		
			Integer underflow can occur when the RTCP length is lesser than than the actual blocks present in Snapdragon	https://www.	
Integer Underflow (Wrap or Wraparoun d)	08-Sep-21	10	blocks present in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Voice & Music, Snapdragon Wearables	qualcomm.co m/company/ product- security/bull etins/august- 2021-bulletin	O-QUA-SD83- 200921/3387
			CVE ID : CVE-2021-1919		
Integer Underflow (Wrap or Wraparoun d)	08-Sep-21	10	Integer underflow can occur due to improper handling of incoming RTCP packets in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Voice & Music, Snapdragon Wearables	https://www. qualcomm.co m/company/ product- security/bull etins/august- 2021-bulletin	O-QUA-SD83- 200921/3388
			CVE ID : CVE-2021-1920		
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	08-Sep-21	10	Possible buffer overflow due to improper validation of device types during P2P search in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile,	https://www. qualcomm.co m/company/ product- security/bull etins/august- 2021-bulletin	0-QUA-SD83- 200921/3389

0-1

1-2

5-6

6-7

7-8

8-9

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking		
			CVE ID : CVE-2021-1972		
sd845_firmw	are			L	
Exposure of Resource to Wrong Sphere	08-Sep-21	2.1	Child process can leak information from parent process due to numeric pids are getting compared and these pid can be reused in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wearables CVE ID : CVE-2021-1904	https://www. qualcomm.co m/company/ product- security/bull etins/august- 2021-bulletin	0-QUA-SD84- 200921/3390
Loop with Unreachable Exit Condition ('Infinite Loop')	08-Sep-21	5	Loop with unreachable exit condition may occur due to improper handling of unsupported input in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Voice & Music, Snapdragon Wearables CVE ID : CVE-2021-1914	https://www. qualcomm.co m/company/ product- security/bull etins/august- 2021-bulletin	0-QUA-SD84- 200921/3391
Out-of- bounds Write	08-Sep-21	10	Possible buffer underflow due to lack of check for negative indices values when processing user provided	https://www. qualcomm.co m/company/ product-	0-QUA-SD84- 200921/3392
CVSS Scoring Sc	ale 0-1	1-2	2-3 3-4 4-5 5-6	6-7 7-8	8-9 9-10

Page 1303 of 1474

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			input in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Voice & Music, Snapdragon Wearables	security/bull etins/august- 2021-bulletin	
			CVE ID : CVE-2021-1916		
Integer Underflow (Wrap or Wraparoun d)	08-Sep-21	10	Integer underflow can occur when the RTCP length is lesser than than the actual blocks present in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Voice & Music, Snapdragon Wearables CVE ID : CVE-2021-1919	https://www. qualcomm.co m/company/ product- security/bull etins/august- 2021-bulletin	0-QUA-SD84- 200921/3393
			Integer underflow can occur		
Integer Underflow (Wrap or Wraparoun d)	08-Sep-21	10	due to improper handling of incoming RTCP packets in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Voice & Music, Snapdragon Wearables	https://www. qualcomm.co m/company/ product- security/bull etins/august- 2021-bulletin	0-QUA-SD84- 200921/3394
Duffor Corre			CVE ID : CVE-2021-1920	https://www.	
Buffer Copy without Checking Size of Input ('Classic	08-Sep-21	10	Possible buffer overflow due to improper validation of device types during P2P search in Snapdragon Auto, Snapdragon Compute,	https://www. qualcomm.co m/company/ product- security/bull	0-QUA-SD84- 200921/3395

0-1

1-2

2-3 3-4 4-5 Page 1304 of 1474 7-8

5-6

6-7

8-9

Buffer Overflow') sd850_firmware		Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking CVE ID : CVE-2021-1972 Loop with unreachable exit	etins/august- 2021-bulletin	
		Loop with upreachable exit		
		Loon with unreachable evit		
Loop with Unreachable Exit Condition ('Infinite Loop')	5	condition may occur due to improper handling of unsupported input in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Voice & Music, Snapdragon Wearables CVE ID : CVE-2021-1914	https://www. qualcomm.co m/company/ product- security/bull etins/august- 2021-bulletin	0-QUA-SD85- 200921/3396
Out-of- bounds 08-Sep-21 Write	10	Possible buffer underflow due to lack of check for negative indices values when processing user provided input in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Voice & Music, Snapdragon Wearables CVE ID : CVE-2021-1916	https://www. qualcomm.co m/company/ product- security/bull etins/august- 2021-bulletin	0-QUA-SD85- 200921/3397
Integer 08-Sep-21	10	Integer underflow can occur	https://www.	0-QUA-SD85-

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Underflow (Wrap or Wraparoun d)			when the RTCP length is lesser than than the actual blocks present in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Voice & Music, Snapdragon Wearables CVE ID : CVE-2021-1919	qualcomm.co m/company/ product- security/bull etins/august- 2021-bulletin	200921/3398
Integer Underflow (Wrap or Wraparoun d)	08-Sep-21	10	Integer underflow can occur due to improper handling of incoming RTCP packets in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Voice & Music, Snapdragon Wearables CVE ID : CVE-2021-1920	https://www. qualcomm.co m/company/ product- security/bull etins/august- 2021-bulletin	0-QUA-SD85- 200921/3399
sd855_firmw	are			<u> </u>	
Exposure of Resource to Wrong Sphere	08-Sep-21	2.1	Child process can leak information from parent process due to numeric pids are getting compared and these pid can be reused in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wearables CVE ID : CVE-2021-1904	https://www. qualcomm.co m/company/ product- security/bull etins/august- 2021-bulletin	0-QUA-SD85- 200921/3400
CVSS Scoring Sca	ale 0-1	1-2	2-3 3-4 4-5 5-6	6-7 7-8	8-9 9-10

3-4 4-5 Page 1306 of 1474

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Loop with Unreachable Exit Condition ('Infinite Loop')	08-Sep-21	5	Loop with unreachable exit condition may occur due to improper handling of unsupported input in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Voice & Music, Snapdragon Wearables CVE ID : CVE-2021-1914	https://www. qualcomm.co m/company/ product- security/bull etins/august- 2021-bulletin	0-QUA-SD85- 200921/3401
Out-of- bounds Write	08-Sep-21	10	Possible buffer underflow due to lack of check for negative indices values when processing user provided input in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Voice & Music, Snapdragon Wearables CVE ID : CVE-2021-1916	https://www. qualcomm.co m/company/ product- security/bull etins/august- 2021-bulletin	0-QUA-SD85- 200921/3402
Integer Underflow (Wrap or Wraparoun d)	08-Sep-21	10	Integer underflow can occur when the RTCP length is lesser than than the actual blocks present in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Voice & Music, Snapdragon Wearables CVE ID : CVE-2021-1919	https://www. qualcomm.co m/company/ product- security/bull etins/august- 2021-bulletin	0-QUA-SD85- 200921/3403

CVSS Scoring Scale0-11-22-3

4-5

5-6

6-7

7-8

8-9

9-10

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Integer Underflow (Wrap or Wraparoun d)	08-Sep-21	10	Integer underflow can occur due to improper handling of incoming RTCP packets in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Voice & Music, Snapdragon Wearables	https://www. qualcomm.co m/company/ product- security/bull etins/august- 2021-bulletin	O-QUA-SD85- 200921/3404
			CVE ID : CVE-2021-1920		
Incorrect Type Conversion or Cast	08-Sep-21	4.6	Incorrect pointer argument passed to trusted application TA could result in un- intended memory operations in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Industrial IOT CVE ID : CVE-2021-1923	https://www. qualcomm.co m/company/ product- security/bull etins/august- 2021-bulletin	O-QUA-SD85- 200921/3405
Exposure of Resource to Wrong Sphere	08-Sep-21	2.1	Lack of strict validation of bootmode can lead to information disclosure in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wearables CVE ID : CVE-2021-1929	https://www. qualcomm.co m/company/ product- security/bull etins/august- 2021-bulletin	0-QUA-SD85- 200921/3406
Improper Restriction of Operations within the Bounds of a	08-Sep-21	3.6	Possible out of bounds read due to incorrect validation of incoming buffer length in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity,	https://www. qualcomm.co m/company/ product- security/bull etins/august-	O-QUA-SD85- 200921/3407

0-1

1-2 2-3 3-4

4-5

5-6

6-7

7-8

8-9

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Memory Buffer			Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile	2021-bulletin	
			CVE ID : CVE-2021-1930		
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	08-Sep-21	10	Possible buffer overflow due to improper validation of device types during P2P search in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Woice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking	https://www. qualcomm.co m/company/ product- security/bull etins/august- 2021-bulletin	0-QUA-SD85- 200921/3408
			CVE ID : CVE-2021-1972		
sd865_5g_fir	mware				ſ
Exposure of Resource to Wrong Sphere	08-Sep-21	2.1	Child process can leak information from parent process due to numeric pids are getting compared and these pid can be reused in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wearables CVE ID : CVE-2021-1904	https://www. qualcomm.co m/company/ product- security/bull etins/august- 2021-bulletin	0-QUA-SD86- 200921/3409
Loop with Unreachable Exit Condition	08-Sep-21	5	Loop with unreachable exit condition may occur due to improper handling of unsupported input in	https://www. qualcomm.co m/company/ product-	0-QUA-SD86- 200921/3410
CVSS Scoring Sc	ale 0-1	1-2	2-3 3-4 4-5 5-6	6-7 7-8	8-9 9-10

Page 1309 of 1474

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
('Infinite Loop')			Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Voice & Music, Snapdragon Wearables CVE ID : CVE-2021-1914	security/bull etins/august- 2021-bulletin	
Out-of- bounds Write	08-Sep-21	10	Possible buffer underflow due to lack of check for negative indices values when processing user provided input in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Voice & Music, Snapdragon Wearables CVE ID : CVE-2021-1916	https://www. qualcomm.co m/company/ product- security/bull etins/august- 2021-bulletin	0-QUA-SD86- 200921/3411
Integer Underflow (Wrap or Wraparoun d)	08-Sep-21	10	Integer underflow can occur when the RTCP length is lesser than than the actual blocks present in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Voice & Music, Snapdragon Wearables CVE ID : CVE-2021-1919	https://www. qualcomm.co m/company/ product- security/bull etins/august- 2021-bulletin	O-QUA-SD86- 200921/3412
Integer Underflow (Wrap or Wraparoun	08-Sep-21	10	Integer underflow can occur due to improper handling of incoming RTCP packets in Snapdragon Auto,	https://www. qualcomm.co m/company/ product-	0-QUA-SD86- 200921/3413

CVSS Scoring Scale	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10
			De		af 1 171					

Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
		Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Voice & Music, Snapdragon Wearables CVE ID : CVE-2021-1920	security/bull etins/august- 2021-bulletin	
08-Sep-21	4.6	Incorrect pointer argument passed to trusted application TA could result in un- intended memory operations in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Industrial IOT CVE ID : CVE-2021-1923	https://www. qualcomm.co m/company/ product- security/bull etins/august- 2021-bulletin	0-QUA-SD86- 200921/3414
08-Sep-21	2.1	Lack of strict validation of bootmode can lead to information disclosure in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wearables CVE ID : CVE-2021-1929	https://www. qualcomm.co m/company/ product- security/bull etins/august- 2021-bulletin	0-QUA-SD86- 200921/3415
08-Sep-21	3.6	Possible out of bounds read due to incorrect validation of incoming buffer length in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile CVE ID : CVE-2021-1930	https://www. qualcomm.co m/company/ product- security/bull etins/august- 2021-bulletin	0-QUA-SD86- 200921/3416
	08-Sep-21 08-Sep-21	08-Sep-21 4.6 08-Sep-21 2.1	Image: construct of the second seco	Image: security is a security is subsective in the security is subsective.08-Sep-213.6Possible out of bo

Page 1311 of 1474

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	08-Sep-21	10	Possible buffer overflow due to improper validation of device types during P2P search in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Woice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking CVE ID : CVE-2021-1972	https://www. qualcomm.co m/company/ product- security/bull etins/august- 2021-bulletin	0-QUA-SD86- 200921/3417
sd870_firmw	are				
Exposure of Resource to Wrong Sphere	08-Sep-21	2.1	Child process can leak information from parent process due to numeric pids are getting compared and these pid can be reused in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables CVE ID : CVE-2021-1904	https://www. qualcomm.co m/company/ product- security/bull etins/august- 2021-bulletin	0-QUA-SD87- 200921/3418
Loop with Unreachable Exit Condition ('Infinite Loop')	08-Sep-21	5	Loop with unreachable exit condition may occur due to improper handling of unsupported input in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT,	https://www. qualcomm.co m/company/ product- security/bull etins/august- 2021-bulletin	0-QUA-SD87- 200921/3419

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Snapdragon IoT, Snapdragon Voice & Music, Snapdragon Wearables		
			CVE ID : CVE-2021-1914		
Out-of- bounds Write	08-Sep-21	10	Possible buffer underflow due to lack of check for negative indices values when processing user provided input in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Voice & Music, Snapdragon Wearables	https://www. qualcomm.co m/company/ product- security/bull etins/august- 2021-bulletin	O-QUA-SD87- 200921/3420
			CVE ID : CVE-2021-1916		
Integer Underflow (Wrap or Wraparoun d)	08-Sep-21	10	Integer underflow can occur when the RTCP length is lesser than than the actual blocks present in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Voice & Music, Snapdragon Wearables	https://www. qualcomm.co m/company/ product- security/bull etins/august- 2021-bulletin	O-QUA-SD87- 200921/3421
			CVE ID : CVE-2021-1919		
Integer Underflow (Wrap or Wraparoun d)	08-Sep-21	10	Integer underflow can occur due to improper handling of incoming RTCP packets in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon	https://www. qualcomm.co m/company/ product- security/bull etins/august- 2021-bulletin	0-QUA-SD87- 200921/3422

0-1

1-2

3-4 2-3 Page 1313 of 1474

4-5

5-6

6-7

7-8

8-9

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Voice & Music, Snapdragon Wearables		
			CVE ID : CVE-2021-1920		
Incorrect Type Conversion or Cast	08-Sep-21	4.6	Incorrect pointer argument passed to trusted application TA could result in un- intended memory operations in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Industrial IOT CVE ID : CVE-2021-1923	https://www. qualcomm.co m/company/ product- security/bull etins/august- 2021-bulletin	0-QUA-SD87- 200921/3423
Exposure of Resource to Wrong Sphere	08-Sep-21	2.1	Lack of strict validation of bootmode can lead to information disclosure in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wearables CVE ID : CVE-2021-1929	https://www. qualcomm.co m/company/ product- security/bull etins/august- 2021-bulletin	0-QUA-SD87- 200921/3424
Improper Restriction of Operations within the Bounds of a Memory Buffer	08-Sep-21	3.6	Possible out of bounds read due to incorrect validation of incoming buffer length in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile CVE ID : CVE-2021-1930	https://www. qualcomm.co m/company/ product- security/bull etins/august- 2021-bulletin	0-QUA-SD87- 200921/3425
Buffer Copy without Checking Size of Input ('Classic CVSS Scoring Sc	08-Sep-21	10	Possible buffer overflow dueto improper validation ofdevice types during P2Psearch in Snapdragon Auto,Snapdragon Compute,2-33-44-55-6	https://www. qualcomm.co m/company/ product- security/bull 6-7 7-8	0-QUA-SD87- 200921/3426 8-9 9-10

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Buffer Overflow')			Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking CVE ID : CVE-2021-1972	etins/august- 2021-bulletin	
sd888_5g_firm	mware				
Exposure of Resource to Wrong Sphere	08-Sep-21	2.1	Child process can leak information from parent process due to numeric pids are getting compared and these pid can be reused in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables CVE ID : CVE-2021-1904	https://www. qualcomm.co m/company/ product- security/bull etins/august- 2021-bulletin	0-QUA-SD88- 200921/3427
Loop with Unreachable Exit Condition ('Infinite Loop')	08-Sep-21	5	Loop with unreachable exit condition may occur due to improper handling of unsupported input in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Voice & Music, Snapdragon Wearables CVE ID : CVE-2021-1914	https://www. qualcomm.co m/company/ product- security/bull etins/august- 2021-bulletin	0-QUA-SD88- 200921/3428
CVSS Scoring Sc	ale 0-1	1-2	2-3 3-4 4-5 5-6	6-7 7-8	8-9 9-10

 3-4
 4-5
 5-6

 Page 1315 of 1474

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Out-of- bounds Write	08-Sep-21	10	Possible buffer underflow due to lack of check for negative indices values when processing user provided input in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Voice & Music, Snapdragon Wearables	https://www. qualcomm.co m/company/ product- security/bull etins/august- 2021-bulletin	0-QUA-SD88- 200921/3429
Integer Underflow (Wrap or Wraparoun d)	08-Sep-21	10	CVE ID : CVE-2021-1916 Integer underflow can occur when the RTCP length is lesser than than the actual blocks present in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Voice & Music, Snapdragon Wearables	https://www. qualcomm.co m/company/ product- security/bull etins/august- 2021-bulletin	0-QUA-SD88- 200921/3430
Integer Underflow (Wrap or Wraparoun d)	08-Sep-21	10	CVE ID : CVE-2021-1919 Integer underflow can occur due to improper handling of incoming RTCP packets in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Voice & Music, Snapdragon Wearables CVE ID : CVE-2021-1920	https://www. qualcomm.co m/company/ product- security/bull etins/august- 2021-bulletin	0-QUA-SD88- 200921/3431
Incorrect	08-Sep-21	<mark>4.6</mark>	Incorrect pointer argument	https://www.	0-QUA-SD88-

 3-4
 4-5
 5-6

 Page 1316 of 1474

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Type Conversion or Cast			passed to trusted application TA could result in un- intended memory operations in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Industrial IOT CVE ID : CVE-2021-1923	qualcomm.co m/company/ product- security/bull etins/august- 2021-bulletin	200921/3432
Exposure of Resource to Wrong Sphere	08-Sep-21	2.1	Lack of strict validation of bootmode can lead to information disclosure in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wearables CVE ID : CVE-2021-1929	https://www. qualcomm.co m/company/ product- security/bull etins/august- 2021-bulletin	0-QUA-SD88- 200921/3433
Improper Restriction of Operations within the Bounds of a Memory Buffer	08-Sep-21	3.6	Possible out of bounds read due to incorrect validation of incoming buffer length in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile CVE ID : CVE-2021-1930	https://www. qualcomm.co m/company/ product- security/bull etins/august- 2021-bulletin	0-QUA-SD88- 200921/3434
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	08-Sep-21	10	Possible buffer overflow due to improper validation of device types during P2P search in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile,	https://www. qualcomm.co m/company/ product- security/bull etins/august- 2021-bulletin	0-QUA-SD88- 200921/3435

0-1 1-2

5-6

6-7

7-8

8-9

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking		
ad000 firmer			CVE ID : CVE-2021-1972		
sd888_firmw	are		Child process can leak		
Exposure of Resource to Wrong Sphere	08-Sep-21	2.1	information from parent process due to numeric pids are getting compared and these pid can be reused in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wearables CVE ID : CVE-2021-1904	https://www. qualcomm.co m/company/ product- security/bull etins/august- 2021-bulletin	0-QUA-SD88- 200921/3436
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	08-Sep-21	10	Possible buffer overflow due to improper validation of device types during P2P search in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Woice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking CVE ID : CVE-2021-1972	https://www. qualcomm.co m/company/ product- security/bull etins/august- 2021-bulletin	0-QUA-SD88- 200921/3437
1 400 6	nware		L	1	1

0-1

1-2

2-3 3-4

4-5

5-6

6-7

7-8

8-9

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Exposure of Resource to Wrong Sphere	08-Sep-21	2.1	Child process can leak information from parent process due to numeric pids are getting compared and these pid can be reused in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wearables CVE ID : CVE-2021-1904	https://www. qualcomm.co m/company/ product- security/bull etins/august- 2021-bulletin	0-QUA-SDA4- 200921/3438
Loop with Unreachable Exit Condition ('Infinite Loop')	08-Sep-21	5	Loop with unreachable exit condition may occur due to improper handling of unsupported input in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Voice & Music, Snapdragon Wearables CVE ID : CVE-2021-1914	https://www. qualcomm.co m/company/ product- security/bull etins/august- 2021-bulletin	0-QUA-SDA4- 200921/3439
Out-of- bounds Write	08-Sep-21	10	Possible buffer underflow due to lack of check for negative indices values when processing user provided input in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Voice & Music, Snapdragon Wearables	https://www. qualcomm.co m/company/ product- security/bull etins/august- 2021-bulletin	0-QUA-SDA4- 200921/3440
CVSS Scoring Sc	ale 0-1	1-2	2-3 3-4 4-5 5-6 Page 1319 of 1474	6-7 7-8	8-9 9-10

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2021-1916		
Out-of- bounds Read	08-Sep-21	3.6	Buffer over read could occur due to incorrect check of buffer size while flashing emmc devices in Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking CVE ID : CVE-2021-1928	https://www. qualcomm.co m/company/ product- security/bull etins/august- 2021-bulletin	O-QUA-SDA4- 200921/3441
Exposure of Resource to Wrong Sphere	08-Sep-21	2.1	Lack of strict validation of bootmode can lead to information disclosure in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wearables CVE ID : CVE-2021-1929	https://www. qualcomm.co m/company/ product- security/bull etins/august- 2021-bulletin	0-QUA-SDA4- 200921/3442
sdm429w_fir	rmware				
Exposure of Resource to Wrong Sphere	08-Sep-21	2.1	Child process can leak information from parent process due to numeric pids are getting compared and these pid can be reused in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music,	https://www. qualcomm.co m/company/ product- security/bull etins/august- 2021-bulletin	O-QUA-SDM4- 200921/3443

CVSS Scoring Scale	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-1
Page 1320 of 1474										

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Snapdragon Wearables		
			CVE ID : CVE-2021-1904		
Loop with Unreachable Exit Condition ('Infinite Loop')	08-Sep-21	5	Loop with unreachable exit condition may occur due to improper handling of unsupported input in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Voice & Music, Snapdragon Wearables CVE ID : CVE-2021-1914	https://www. qualcomm.co m/company/ product- security/bull etins/august- 2021-bulletin	0-QUA-SDM4- 200921/3444
Out-of- bounds Write	08-Sep-21	10	Possible buffer underflow due to lack of check for negative indices values when processing user provided input in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Voice & Music, Snapdragon Wearables CVE ID : CVE-2021-1916	https://www. qualcomm.co m/company/ product- security/bull etins/august- 2021-bulletin	O-QUA-SDM4- 200921/3445
Buffer Copy without Checking Size of Input ('Classic Buffer	08-Sep-21	10	Possible buffer overflow due to improper validation of device types during P2P search in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT,	https://www. qualcomm.co m/company/ product- security/bull etins/august-	0-QUA-SDM4- 200921/3446
Overflow')			Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music,	2021-bulletin	

1-2 2-3

0-1

5-6

6-7

7-8

8-9

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking		
			CVE ID : CVE-2021-1972		
sdm630_firm	iware				
Exposure of Resource to Wrong Sphere	08-Sep-21	2.1	Child process can leak information from parent process due to numeric pids are getting compared and these pid can be reused in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wearables CVE ID : CVE-2021-1904	https://www. qualcomm.co m/company/ product- security/bull etins/august- 2021-bulletin	0-QUA-SDM6- 200921/3447
Loop with Unreachable Exit Condition ('Infinite Loop')	08-Sep-21	5	Loop with unreachable exit condition may occur due to improper handling of unsupported input in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Voice & Music, Snapdragon Wearables CVE ID : CVE-2021-1914	https://www. qualcomm.co m/company/ product- security/bull etins/august- 2021-bulletin	0-QUA-SDM6- 200921/3448
Out-of- bounds Write	08-Sep-21	10	Possible buffer underflow due to lack of check for negative indices values when processing user provided input in Snapdragon Auto,	https://www. qualcomm.co m/company/ product- security/bull	0-QUA-SDM6- 200921/3449
CVSS Scoring Sc	ale 0-1	1-2	2-3 3-4 4-5 5-6	6-7 7-8	8-9 9-10

Page 1322 of 1474

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Voice & Music, Snapdragon Wearables	etins/august- 2021-bulletin	
			CVE ID : CVE-2021-1916		
Integer Underflow (Wrap or Wraparoun d)	08-Sep-21	10	Integer underflow can occur when the RTCP length is lesser than than the actual blocks present in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Voice & Music, Snapdragon Wearables CVE ID : CVE-2021-1919	https://www. qualcomm.co m/company/ product- security/bull etins/august- 2021-bulletin	0-QUA-SDM6- 200921/3450
Integer Underflow (Wrap or Wraparoun d)	08-Sep-21	10	Integer underflow can occur due to improper handling of incoming RTCP packets in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Voice & Music, Snapdragon Wearables CVE ID : CVE-2021-1920	https://www. qualcomm.co m/company/ product- security/bull etins/august- 2021-bulletin	0-QUA-SDM6- 200921/3451
Buffer Copy without Checking Size of Input ('Classic Buffer	08-Sep-21	10	Possible buffer overflow due to improper validation of device types during P2P search in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity,	https://www. qualcomm.co m/company/ product- security/bull etins/august-	0-QUA-SDM6- 200921/3452

0-1

1-2 2-3 3-4

4-5

5-6

6-7

7-8

8-9

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Overflow')			Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking CVE ID : CVE-2021-1972	2021-bulletin	
sdm830_firm	ware				
Exposure of Resource to Wrong Sphere	08-Sep-21	2.1	Child process can leak information from parent process due to numeric pids are getting compared and these pid can be reused in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wearables CVE ID : CVE-2021-1904	https://www. qualcomm.co m/company/ product- security/bull etins/august- 2021-bulletin	0-QUA-SDM8- 200921/3453
Incorrect Type Conversion or Cast	08-Sep-21	4.6	Incorrect pointer argument passed to trusted application TA could result in un- intended memory operations in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Industrial IOT CVE ID : CVE-2021-1923	https://www. qualcomm.co m/company/ product- security/bull etins/august- 2021-bulletin	0-QUA-SDM8- 200921/3454
Exposure of Resource to Wrong Sphere	08-Sep-21	2.1	Lack of strict validation of bootmode can lead to information disclosure in Snapdragon Auto, Snapdragon Compute,	https://www. qualcomm.co m/company/ product- security/bull	0-QUA-SDM8- 200921/3455
CVSS Scoring Sc	ale 0-1	1-2	2-3 3-4 4-5 5-6	6-7 7-8	8-9 <mark>9-10</mark>

Page 1324 of 1474

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wearables	etins/august- 2021-bulletin	
			CVE ID : CVE-2021-1929		
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	08-Sep-21	10	Possible buffer overflow due to improper validation of device types during P2P search in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Woice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking CVE ID : CVE-2021-1972	https://www. qualcomm.co m/company/ product- security/bull etins/august- 2021-bulletin	0-QUA-SDM8- 200921/3456
sdw2500_firm	nware				
Exposure of Resource to Wrong Sphere	08-Sep-21	2.1	Child process can leak information from parent process due to numeric pids are getting compared and these pid can be reused in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables CVE ID : CVE-2021-1904	https://www. qualcomm.co m/company/ product- security/bull etins/august- 2021-bulletin	0-QUA-SDW2- 200921/3457
Loop with Unreachable	08-Sep-21	5	Loop with unreachable exit condition may occur due to	https://www. qualcomm.co	0-QUA-SDW2- 200921/3458

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Exit Condition ('Infinite Loop')			improper handling of unsupported input in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Voice & Music, Snapdragon Wearables CVE ID : CVE-2021-1914	m/company/ product- security/bull etins/august- 2021-bulletin	
Out-of- bounds Write	08-Sep-21	10	Possible buffer underflow due to lack of check for negative indices values when processing user provided input in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Voice & Music, Snapdragon Wearables CVE ID : CVE-2021-1916	https://www. qualcomm.co m/company/ product- security/bull etins/august- 2021-bulletin	0-QUA-SDW2- 200921/3459
Integer Underflow (Wrap or Wraparoun d)	08-Sep-21	10	Integer underflow can occur when the RTCP length is lesser than than the actual blocks present in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Voice & Music, Snapdragon Wearables CVE ID : CVE-2021-1919	https://www. qualcomm.co m/company/ product- security/bull etins/august- 2021-bulletin	0-QUA-SDW2- 200921/3460
Integer Underflow	08-Sep-21	10	Integer underflow can occur due to improper handling of	https://www. qualcomm.co	0-QUA-SDW2- 200921/3461
CVSS Scoring Sc	ale 0-1	1-2	2-3 3-4 4-5 5-6 Page 1326 of 1474	6-7 7-8	8-9 9-10

3-4 4-5 Page 1326 of 1474

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
(Wrap or Wraparoun d)			incoming RTCP packets in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Voice & Music, Snapdragon Wearables CVE ID : CVE-2021-1920	m/company/ product- security/bull etins/august- 2021-bulletin	
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	08-Sep-21	10	Possible buffer overflow due to improper validation of device types during P2P search in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Woice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking CVE ID : CVE-2021-1972	https://www. qualcomm.co m/company/ product- security/bull etins/august- 2021-bulletin	0-QUA-SDW2- 200921/3462
sdx12_firmw	vare				
Exposure of Resource to Wrong Sphere	08-Sep-21	2.1	Child process can leak information from parent process due to numeric pids are getting compared and these pid can be reused in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music,	https://www. qualcomm.co m/company/ product- security/bull etins/august- 2021-bulletin	O-QUA-SDX1- 200921/3463

CVSS Scoring Scale	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10
	Page 1327 of 1474									

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Snapdragon Wearables		
			CVE ID : CVE-2021-1904		
Loop with Unreachable Exit Condition ('Infinite Loop')	08-Sep-21	5	Loop with unreachable exit condition may occur due to improper handling of unsupported input in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Voice & Music, Snapdragon Wearables	https://www. qualcomm.co m/company/ product- security/bull etins/august- 2021-bulletin	O-QUA-SDX1- 200921/3464
			CVE ID : CVE-2021-1914		
Out-of- bounds Write	08-Sep-21	10	Possible buffer underflow due to lack of check for negative indices values when processing user provided input in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Voice & Music, Snapdragon Wearables	https://www. qualcomm.co m/company/ product- security/bull etins/august- 2021-bulletin	O-QUA-SDX1- 200921/3465
			CVE ID : CVE-2021-1916		
Integer Underflow (Wrap or Wraparoun d)	08-Sep-21	10	Integer underflow can occur when the RTCP length is lesser than than the actual blocks present in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Voice & Music, Snapdragon	https://www. qualcomm.co m/company/ product- security/bull etins/august- 2021-bulletin	O-QUA-SDX1- 200921/3466

0-1

1-2

5-6

6-7

7-8

8-9

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Wearables		
			CVE ID : CVE-2021-1919		
Integer Underflow (Wrap or Wraparoun d)	08-Sep-21	10	Integer underflow can occur due to improper handling of incoming RTCP packets in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Voice & Music, Snapdragon Wearables	https://www. qualcomm.co m/company/ product- security/bull etins/august- 2021-bulletin	0-QUA-SDX1- 200921/3467
			CVE ID : CVE-2021-1920		
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	08-Sep-21	10	Possible buffer overflow due to improper validation of device types during P2P search in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Woice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking CVE ID : CVE-2021-1972	https://www. qualcomm.co m/company/ product- security/bull etins/august- 2021-bulletin	0-QUA-SDX1- 200921/3468
sdx20m_firm	ware				
Exposure of Resource to Wrong Sphere	08-Sep-21	2.1	Child process can leak information from parent process due to numeric pids are getting compared and these pid can be reused in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity,	https://www. qualcomm.co m/company/ product- security/bull etins/august- 2021-bulletin	0-QUA-SDX2- 200921/3469
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 & CVE ID	Patch	NCIIPC ID		
			Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables CVE ID : CVE-2021-1904				
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	08-Sep-21	10	Possible buffer overflow due to improper validation of device types during P2P search in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Industrial IOT, Snapdragon Woice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking CVE ID : CVE-2021-1972	https://www. qualcomm.co m/company/ product- security/bull etins/august- 2021-bulletin	0-QUA-SDX2- 200921/3470		
sdx20_firmw	<u> </u>						
Exposure of Resource to Wrong Sphere	08-Sep-21	2.1	Child process can leak information from parent process due to numeric pids are getting compared and these pid can be reused in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wearables CVE ID : CVE-2021-1904	https://www. qualcomm.co m/company/ product- security/bull etins/august- 2021-bulletin	O-QUA-SDX2- 200921/3471		
Loop with Unreachable	08-Sep-21	5	Loop with unreachable exit condition may occur due to	https://www. qualcomm.co	0-QUA-SDX2- 200921/3472		

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID	
Exit Condition ('Infinite Loop')			improper handling of unsupported input in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Voice & Music, Snapdragon Wearables CVE ID : CVE-2021-1914	m/company/ product- security/bull etins/august- 2021-bulletin		
Out-of- bounds Write	08-Sep-21	10	Possible buffer underflow due to lack of check for negative indices values when processing user provided input in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Voice & Music, Snapdragon Wearables CVE ID : CVE-2021-1916	https://www. qualcomm.co m/company/ product- security/bull etins/august- 2021-bulletin	0-QUA-SDX2- 200921/3473	
Integer Underflow (Wrap or Wraparoun d)	nderflow Vrap or 08-Sep-21 10 raparoun		Integer underflow can occur when the RTCP length is lesser than than the actual blocks present in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Voice & Music, Snapdragon Wearables CVE ID : CVE-2021-1919	https://www. qualcomm.co m/company/ product- security/bull etins/august- 2021-bulletin	O-QUA-SDX2- 200921/3474	
Integer	08-Sep-21	10	Integer underflow can occur due to improper handling of	https://www. qualcomm.co	0-QUA-SDX2- 200921/3475	

 3-4
 4-5
 5-6
 6-7

 Page 1331 of 1474

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID	
(Wrap or Wraparoun d)			incoming RTCP packets in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Voice & Music, Snapdragon Wearables CVE ID : CVE-2021-1920	m/company/ product- security/bull etins/august- 2021-bulletin		
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	08-Sep-21	10	Possible buffer overflow due to improper validation of device types during P2P search in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Woice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking CVE ID : CVE-2021-1972	https://www. qualcomm.co m/company/ product- security/bull etins/august- 2021-bulletin	0-QUA-SDX2- 200921/3476	
sdx24_firmw	vare					
Exposure of Resource to Wrong Sphere	08-Sep-21	2.1	Child process can leak information from parent process due to numeric pids are getting compared and these pid can be reused in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music,	https://www. qualcomm.co m/company/ product- security/bull etins/august- 2021-bulletin	O-QUA-SDX2- 200921/3477	

CVSS Scoring Scale	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10
Page 1332 of 1474										

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Snapdragon Wearables		
			CVE ID : CVE-2021-1904		
Loop with Unreachable Exit Condition ('Infinite Loop')	08-Sep-21	5	Loop with unreachable exit condition may occur due to improper handling of unsupported input in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Voice & Music, Snapdragon Wearables	https://www. qualcomm.co m/company/ product- security/bull etins/august- 2021-bulletin	O-QUA-SDX2- 200921/3478
			CVE ID : CVE-2021-1914		
Out-of- bounds Write	08-Sep-21	10	Possible buffer underflow due to lack of check for negative indices values when processing user provided input in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Voice & Music, Snapdragon Wearables	https://www. qualcomm.co m/company/ product- security/bull etins/august- 2021-bulletin	0-QUA-SDX2- 200921/3479
			CVE ID : CVE-2021-1916		
Integer Underflow (Wrap or Wraparoun d)	08-Sep-21	10	Integer underflow can occur when the RTCP length is lesser than than the actual blocks present in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Voice & Music, Snapdragon	https://www. qualcomm.co m/company/ product- security/bull etins/august- 2021-bulletin	O-QUA-SDX2- 200921/3480

0-1

1-2

2-3 3-4 4-5 Page 1333 of 1474

5-6

6-7

7-8

8-9

Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
		Wearables		
		CVE ID : CVE-2021-1919		
08-Sep-21	10	Integer underflow can occur due to improper handling of incoming RTCP packets in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Voice & Music, Snapdragon Wearables	https://www. qualcomm.co m/company/ product- security/bull etins/august- 2021-bulletin	0-QUA-SDX2- 200921/3481
		CVE ID : CVE-2021-1920		
08-Sep-21	4.6	Incorrect pointer argument passed to trusted application TA could result in un- intended memory operations in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Industrial IOT CVE ID : CVE-2021-1923	https://www. qualcomm.co m/company/ product- security/bull etins/august- 2021-bulletin	0-QUA-SDX2- 200921/3482
08-Sep-21	3.6	Possible out of bounds read due to incorrect validation of incoming buffer length in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile CVE ID : CVE-2021-1930	https://www. qualcomm.co m/company/ product- security/bull etins/august- 2021-bulletin	0-QUA-SDX2- 200921/3483
08-Sep-21	10	Possible buffer overflow due to improper validation of device types during P2P search in Snapdragon Auto, Snapdragon Compute,	https://www. qualcomm.co m/company/ product- security/bull	0-QUA-SDX2- 200921/3484
	08-Sep-21 08-Sep-21	Image: select of the select	Image: constraint of the second sec	Image: Note of the second state of the second stat

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID		
Buffer Overflow')			Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking CVE ID : CVE-2021-1972	etins/august- 2021-bulletin			
sdx50m_firm	ware				L		
Exposure of Resource to Wrong Sphere	08-Sep-21	2.1	Child process can leak information from parent process due to numeric pids are getting compared and these pid can be reused in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wearables CVE ID : CVE-2021-1904	https://www. qualcomm.co m/company/ product- security/bull etins/august- 2021-bulletin	0-QUA-SDX5- 200921/3485		
Loop with Unreachable Exit Condition ('Infinite Loop')	08-Sep-21	5	Loop with unreachable exit condition may occur due to improper handling of unsupported input in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Voice & Music, Snapdragon Wearables CVE ID : CVE-2021-1914	https://www. qualcomm.co m/company/ product- security/bull etins/august- 2021-bulletin	0-QUA-SDX5- 200921/3486		
CVSS Scoring Scale 0-1 1-2 2-3 3-4 4-5 5-6 6-7 7-8 8-9 9-10							

Sep-21	10	Possible buffer underflow due to lack of check for negative indices values when processing user provided input in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT,	https://www. qualcomm.co m/company/ product-	O-QUA-SDX5-
		Snapdragon IoT, Snapdragon Voice & Music, Snapdragon Wearables	security/bull etins/august- 2021-bulletin	200921/3487
Sep-21	10	Integer underflow can occur when the RTCP length is lesser than than the actual blocks present in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Voice & Music, Snapdragon Wearables	https://www. qualcomm.co m/company/ product- security/bull etins/august- 2021-bulletin	0-QUA-SDX5- 200921/3488
		CVE ID : CVE-2021-1919		
Sep-21	10	Integer underflow can occur due to improper handling of incoming RTCP packets in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Voice & Music, Snapdragon Wearables CVE ID : CVE-2021-1920	https://www. qualcomm.co m/company/ product- security/bull etins/august- 2021-bulletin	0-QUA-SDX5- 200921/3489
Sep-21	4.6	Incorrect pointer argument	https://www.	O-QUA-SDX5-
	Sep-21	ep-21 10	Pep-2110lesser than than the actual blocks present in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Voice & Music, Snapdragon WearablesVer ID : CVE-2021-1919Integer underflow can occur due to improper handling of incoming RTCP packets in Snapdragon Consumer IOT, Snapdragon Consumer IOT, Snapdragon Auto, Snapdragon Compute, Snapdragon Compute, Snapdragon Industrial IOT, Snapdragon Consumer IOT, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Industrial IOT, Snapdragon Industrial IOT, Snapdragon Industrial IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Voice & Music, Snapdragon Wearablesep-214.6Incorrect pointer argument	Pep-21Integer underflow can occur when the RTCP length is lesser than than the actual blocks present in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Voice & Music, Snapdragon Snapdragon Connectivity, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Voice & Music, Snap

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Type Conversion or Cast			passed to trusted application TA could result in un- intended memory operations in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Industrial IOT CVE ID : CVE-2021-1923	qualcomm.co m/company/ product- security/bull etins/august- 2021-bulletin	200921/3490
Exposure of Resource to Wrong Sphere	08-Sep-21	2.1	Lack of strict validation of bootmode can lead to information disclosure in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wearables CVE ID : CVE-2021-1929	https://www. qualcomm.co m/company/ product- security/bull etins/august- 2021-bulletin	O-QUA-SDX5- 200921/3491
Improper Restriction of Operations within the Bounds of a Memory Buffer	08-Sep-21	3.6	Possible out of bounds read due to incorrect validation of incoming buffer length in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile CVE ID : CVE-2021-1930	https://www. qualcomm.co m/company/ product- security/bull etins/august- 2021-bulletin	0-QUA-SDX5- 200921/3492
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	08-Sep-21	10	Possible buffer overflow due to improper validation of device types during P2P search in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile,	https://www. qualcomm.co m/company/ product- security/bull etins/august- 2021-bulletin	0-QUA-SDX5- 200921/3493

0-1

1-2

4-5

5-6

6-7

7-8

8-9

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking		
			CVE ID : CVE-2021-1972		
sdx55m_firm	ware			I	I
Exposure of Resource to Wrong Sphere	08-Sep-21	2.1	Child process can leak information from parent process due to numeric pids are getting compared and these pid can be reused in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wearables CVE ID : CVE-2021-1904	https://www. qualcomm.co m/company/ product- security/bull etins/august- 2021-bulletin	0-QUA-SDX5- 200921/3494
Loop with Unreachable Exit Condition ('Infinite Loop')	08-Sep-21	5	Loop with unreachable exit condition may occur due to improper handling of unsupported input in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Voice & Music, Snapdragon Wearables CVE ID : CVE-2021-1914	https://www. qualcomm.co m/company/ product- security/bull etins/august- 2021-bulletin	0-QUA-SDX5- 200921/3495
Out-of- bounds Write	08-Sep-21	10	Possible buffer underflow due to lack of check for negative indices values when processing user provided	https://www. qualcomm.co m/company/ product-	0-QUA-SDX5- 200921/3496
CVSS Scoring Sc	ale 0-1	1-2	2-3 3-4 4-5 5-6	6-7 7-8	8-9 9-10

Page 1338 of 1474

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			input in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Voice & Music, Snapdragon Wearables	security/bull etins/august- 2021-bulletin	
Integer Underflow (Wrap or Wraparoun d)	08-Sep-21	10	CVE ID : CVE-2021-1916 Integer underflow can occur when the RTCP length is lesser than than the actual blocks present in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Voice & Music, Snapdragon Wearables CVE ID : CVE-2021-1919	https://www. qualcomm.co m/company/ product- security/bull etins/august- 2021-bulletin	O-QUA-SDX5- 200921/3497
Integer Underflow (Wrap or Wraparoun d)	08-Sep-21	10	Integer underflow can occur due to improper handling of incoming RTCP packets in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Voice & Music, Snapdragon Wearables CVE ID : CVE-2021-1920	https://www. qualcomm.co m/company/ product- security/bull etins/august- 2021-bulletin	0-QUA-SDX5- 200921/3498
Incorrect Type Conversion or Cast	08-Sep-21	4.6	Incorrect pointer argument passed to trusted application TA could result in un- intended memory operations in Snapdragon Auto,	https://www. qualcomm.co m/company/ product- security/bull	0-QUA-SDX5- 200921/3499

[CVSS Scoring Scale	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10
-				Pa	ge 1339	of 1474					

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Snapdragon Compute, Snapdragon Connectivity, Snapdragon Industrial IOT CVE ID : CVE-2021-1923	etins/august- 2021-bulletin	
Exposure of Resource to Wrong Sphere	08-Sep-21	2.1	Lack of strict validation of bootmode can lead to information disclosure in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wearables	https://www. qualcomm.co m/company/ product- security/bull etins/august- 2021-bulletin	O-QUA-SDX5- 200921/3500
Improper Restriction of Operations within the Bounds of a Memory Buffer	08-Sep-21	3.6	CVE ID : CVE-2021-1929 Possible out of bounds read due to incorrect validation of incoming buffer length in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile CVE ID : CVE-2021-1930	https://www. qualcomm.co m/company/ product- security/bull etins/august- 2021-bulletin	0-QUA-SDX5- 200921/3501
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	08-Sep-21	10	Possible buffer overflow due to improper validation of device types during P2P search in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Woice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and	https://www. qualcomm.co m/company/ product- security/bull etins/august- 2021-bulletin	0-QUA-SDX5- 200921/3502

0-1

1-2

7-8

5-6

6-7

8-9

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID			
			Networking					
			CVE ID : CVE-2021-1972					
sdx55_firmware								
Exposure of Resource to Wrong Sphere	08-Sep-21	2.1	Child process can leak information from parent process due to numeric pids are getting compared and these pid can be reused in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wearables CVE ID : CVE-2021-1904	https://www. qualcomm.co m/company/ product- security/bull etins/august- 2021-bulletin	O-QUA-SDX5- 200921/3503			
Loop with Unreachable Exit Condition ('Infinite Loop')	08-Sep-21	5	Loop with unreachable exit condition may occur due to improper handling of unsupported input in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Voice & Music, Snapdragon Wearables CVE ID : CVE-2021-1914	https://www. qualcomm.co m/company/ product- security/bull etins/august- 2021-bulletin	0-QUA-SDX5- 200921/3504			
Out-of- bounds Write	08-Sep-21	10	Possible buffer underflow due to lack of check for negative indices values when processing user provided input in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT,	https://www. qualcomm.co m/company/ product- security/bull etins/august- 2021-bulletin	0-QUA-SDX5- 200921/3505			
CVSS Scoring Sc	ale 0-1	1-2	2-3 3-4 4-5 5-6	6-7 7-8	8-9 9-10			

Page 1341 of 1474

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Voice & Music, Snapdragon Wearables		
			CVE ID : CVE-2021-1916		
Integer Underflow (Wrap or Wraparoun d)	08-Sep-21	10	Integer underflow can occur when the RTCP length is lesser than than the actual blocks present in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Voice & Music, Snapdragon Wearables CVE ID : CVE-2021-1919	https://www. qualcomm.co m/company/ product- security/bull etins/august- 2021-bulletin	0-QUA-SDX5- 200921/3506
Integer Underflow (Wrap or Wraparoun d)	08-Sep-21	10	Integer underflow can occur due to improper handling of incoming RTCP packets in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Voice & Music, Snapdragon Wearables	https://www. qualcomm.co m/company/ product- security/bull etins/august- 2021-bulletin	0-QUA-SDX5- 200921/3507
			CVE ID : CVE-2021-1920		
Incorrect Type Conversion or Cast	08-Sep-21	4.6	Incorrect pointer argument passed to trusted application TA could result in un- intended memory operations in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Industrial IOT CVE ID : CVE-2021-1923	https://www. qualcomm.co m/company/ product- security/bull etins/august- 2021-bulletin	0-QUA-SDX5- 200921/3508
CVSS Scoring Sc	ale 0-1	1-2	2-3 3-4 4-5 5-6 Page 1342 of 1474	6-7 7-8	8-9 9-10

Page 1342 of 1474

Wrong Sphere Improper Restriction of Operations	08-Sep-21	2.1	Lack of strict validation of bootmode can lead to information disclosure in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wearables CVE ID : CVE-2021-1929	https://www. qualcomm.co m/company/ product- security/bull etins/august- 2021-bulletin	0-QUA-SDX5- 200921/3509
Restriction of Operations					1
within the Bounds of a Memory Buffer	08-Sep-21	3.6	Possible out of bounds read due to incorrect validation of incoming buffer length in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile CVE ID : CVE-2021-1930	https://www. qualcomm.co m/company/ product- security/bull etins/august- 2021-bulletin	O-QUA-SDX5- 200921/3510
Buffer Copy without Checking Size of Input (('Classic Buffer Overflow')	08-Sep-21	10	Possible buffer overflow due to improper validation of device types during P2P search in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Industrial IOT, Snapdragon Woile, Snapdragon Woice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking CVE ID : CVE-2021-1972	https://www. qualcomm.co m/company/ product- security/bull etins/august- 2021-bulletin	O-QUA-SDX5- 200921/3511
sdxr1_firmwar	re				
Exposure of (08-Sep-21	2.1	Child process can leak	https://www.	O-QUA-SDXR-

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Resource to Wrong Sphere			information from parent process due to numeric pids are getting compared and these pid can be reused in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wearables CVE ID : CVE-2021-1904	qualcomm.co m/company/ product- security/bull etins/august- 2021-bulletin	200921/3512
Loop with Unreachable Exit Condition ('Infinite Loop')	08-Sep-21	5	Loop with unreachable exit condition may occur due to improper handling of unsupported input in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Voice & Music, Snapdragon Wearables CVE ID : CVE-2021-1914	https://www. qualcomm.co m/company/ product- security/bull etins/august- 2021-bulletin	O-QUA-SDXR- 200921/3513
Out-of- bounds Write	08-Sep-21	10	Possible buffer underflow due to lack of check for negative indices values when processing user provided input in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Voice & Music, Snapdragon Wearables	https://www. qualcomm.co m/company/ product- security/bull etins/august- 2021-bulletin	O-QUA-SDXR- 200921/3514

CVSS Scoring Scale	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10
			Pa	nge 1344 (of 1474					

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2021-1916		
Integer Underflow (Wrap or Wraparoun d)	08-Sep-21	10	Integer underflow can occur when the RTCP length is lesser than than the actual blocks present in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Voice & Music, Snapdragon Wearables CVE ID : CVE-2021-1919	https://www. qualcomm.co m/company/ product- security/bull etins/august- 2021-bulletin	0-QUA-SDXR- 200921/3515
Integer Underflow (Wrap or Wraparoun d)	08-Sep-21	10	Integer underflow can occur due to improper handling of incoming RTCP packets in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Voice & Music, Snapdragon Wearables CVE ID : CVE-2021-1920	https://www. qualcomm.co m/company/ product- security/bull etins/august- 2021-bulletin	O-QUA-SDXR- 200921/3516
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	08-Sep-21	10	Possible buffer overflow due to improper validation of device types during P2P search in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Woice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and	https://www. qualcomm.co m/company/ product- security/bull etins/august- 2021-bulletin	0-QUA-SDXR- 200921/3517

CVSS Scoring Scale	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10
			Ра	ige 1345	of 1474					

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Networking		
			CVE ID : CVE-2021-1972		
sdxr2_5g_firm	nware				
Exposure of Resource to Wrong Sphere	08-Sep-21	2.1	Child process can leak information from parent process due to numeric pids are getting compared and these pid can be reused in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wearables CVE ID : CVE-2021-1904	https://www. qualcomm.co m/company/ product- security/bull etins/august- 2021-bulletin	0-QUA-SDXR- 200921/3518
Loop with Unreachable Exit Condition ('Infinite Loop')	08-Sep-21	5	Loop with unreachable exit condition may occur due to improper handling of unsupported input in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Voice & Music, Snapdragon Wearables CVE ID : CVE-2021-1914	https://www. qualcomm.co m/company/ product- security/bull etins/august- 2021-bulletin	0-QUA-SDXR- 200921/3519
Out-of- bounds Write	08-Sep-21	10	Possible buffer underflow due to lack of check for negative indices values when processing user provided input in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT,	https://www. qualcomm.co m/company/ product- security/bull etins/august- 2021-bulletin	0-QUA-SDXR- 200921/3520
CVSS Scoring Sc	ale 0-1	1-2	2-3 3-4 4-5 5-6	6-7 7-8	8-9 9-10

Page 1346 of 1474

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Voice & Music, Snapdragon Wearables		
			CVE ID : CVE-2021-1916		
Integer Underflow (Wrap or Wraparoun d)	08-Sep-21	10	Integer underflow can occur when the RTCP length is lesser than than the actual blocks present in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Voice & Music, Snapdragon Wearables CVE ID : CVE-2021-1919	https://www. qualcomm.co m/company/ product- security/bull etins/august- 2021-bulletin	0-QUA-SDXR- 200921/3521
Integer Underflow (Wrap or Wraparoun d)	08-Sep-21	10	Integer underflow can occur due to improper handling of incoming RTCP packets in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Voice & Music, Snapdragon Wearables CVE ID : CVE-2021-1920	https://www. qualcomm.co m/company/ product- security/bull etins/august- 2021-bulletin	0-QUA-SDXR- 200921/3522
Incorrect Type Conversion or Cast	08-Sep-21	4.6	Incorrect pointer argument passed to trusted application TA could result in un- intended memory operations in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Industrial IOT CVE ID : CVE-2021-1923	https://www. qualcomm.co m/company/ product- security/bull etins/august- 2021-bulletin	0-QUA-SDXR- 200921/3523
CVSS Scoring Sc	ale 0-1	1-2	2-3 3-4 4-5 5-6 Page 1347 of 1474	6-7 7-8	8-9 9-10

Page 1347 of 1474

			Description & CVE ID	Patch	NCIIPC ID					
Exposure of Resource to Wrong Sphere	08-Sep-21	2.1	Lack of strict validation of bootmode can lead to information disclosure in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wearables CVE ID : CVE-2021-1929	https://www. qualcomm.co m/company/ product- security/bull etins/august- 2021-bulletin	0-QUA-SDXR- 200921/3524					
Improper Restriction of Operations within the Bounds of a Memory Buffer	08-Sep-21	3.6	Possible out of bounds read due to incorrect validation of incoming buffer length in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile CVE ID : CVE-2021-1930	https://www. qualcomm.co m/company/ product- security/bull etins/august- 2021-bulletin	0-QUA-SDXR- 200921/3525					
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	08-Sep-21	10	Possible buffer overflow due to improper validation of device types during P2P search in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Industrial IOT, Snapdragon Woice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking CVE ID : CVE-2021-1972	https://www. qualcomm.co m/company/ product- security/bull etins/august- 2021-bulletin	O-QUA-SDXR- 200921/3526					
sd 455 firm	sd_455_firmware									
3u_455_mm		-		https://www.	0-QUA-SD_4-					

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Resource to Wrong Sphere			information from parent process due to numeric pids are getting compared and these pid can be reused in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wearables CVE ID : CVE-2021-1904	qualcomm.co m/company/ product- security/bull etins/august- 2021-bulletin	200921/3527
Loop with Unreachable Exit Condition ('Infinite Loop')	08-Sep-21	5	Loop with unreachable exit condition may occur due to improper handling of unsupported input in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Voice & Music, Snapdragon Wearables CVE ID : CVE-2021-1914	https://www. qualcomm.co m/company/ product- security/bull etins/august- 2021-bulletin	0-QUA-SD_4- 200921/3528
Out-of- bounds Write	08-Sep-21	10	Possible buffer underflow due to lack of check for negative indices values when processing user provided input in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Voice & Music, Snapdragon Wearables	https://www. qualcomm.co m/company/ product- security/bull etins/august- 2021-bulletin	0-QUA-SD_4- 200921/3529

CVSS Scoring Scale	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10
			Pa	ige 1349 (of 1474					

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2021-1916		
Integer Underflow (Wrap or Wraparoun d)	08-Sep-21	10	Integer underflow can occur when the RTCP length is lesser than than the actual blocks present in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Voice & Music, Snapdragon Wearables CVE ID : CVE-2021-1919	https://www. qualcomm.co m/company/ product- security/bull etins/august- 2021-bulletin	0-QUA-SD_4- 200921/3530
Integer Underflow (Wrap or Wraparoun d)	08-Sep-21	10	Integer underflow can occur due to improper handling of incoming RTCP packets in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Voice & Music, Snapdragon Wearables CVE ID : CVE-2021-1920	https://www. qualcomm.co m/company/ product- security/bull etins/august- 2021-bulletin	0-QUA-SD_4- 200921/3531
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	08-Sep-21	10	Possible buffer overflow due to improper validation of device types during P2P search in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Woice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and	https://www. qualcomm.co m/company/ product- security/bull etins/august- 2021-bulletin	0-QUA-SD_4- 200921/3532

CVSS Scoring Scale	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10
			Ра	ige 1350	of 1474					

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Networking		
			CVE ID : CVE-2021-1972		
sd_636_firmv	vare				
Exposure of Resource to Wrong Sphere	08-Sep-21	2.1	Child process can leak information from parent process due to numeric pids are getting compared and these pid can be reused in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wearables CVE ID : CVE-2021-1904	https://www. qualcomm.co m/company/ product- security/bull etins/august- 2021-bulletin	0-QUA-SD_6- 200921/3533
Loop with Unreachable Exit Condition ('Infinite Loop')	08-Sep-21	5	Loop with unreachable exit condition may occur due to improper handling of unsupported input in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Voice & Music, Snapdragon Wearables CVE ID : CVE-2021-1914	https://www. qualcomm.co m/company/ product- security/bull etins/august- 2021-bulletin	0-QUA-SD_6- 200921/3534
Out-of- bounds Write	08-Sep-21	10	Possible buffer underflow due to lack of check for negative indices values when processing user provided input in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT,	https://www. qualcomm.co m/company/ product- security/bull etins/august- 2021-bulletin	0-QUA-SD_6- 200921/3535
CVSS Scoring Sc	ale 0-1	1-2	2-3 3-4 4-5 5-6	6-7 7-8	8-9 9-10

Page 1351 of 1474

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Voice & Music, Snapdragon Wearables CVE ID : CVE-2021-1916		
Integer Underflow (Wrap or Wraparoun d)	08-Sep-21	10	Integer underflow can occur when the RTCP length is lesser than than the actual blocks present in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Voice & Music, Snapdragon Wearables	https://www. qualcomm.co m/company/ product- security/bull etins/august- 2021-bulletin	0-QUA-SD_6- 200921/3536
Integer Underflow (Wrap or Wraparoun d)	08-Sep-21	10	CVE ID : CVE-2021-1919 Integer underflow can occur due to improper handling of incoming RTCP packets in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Voice & Music, Snapdragon Wearables CVE ID : CVE-2021-1920	https://www. qualcomm.co m/company/ product- security/bull etins/august- 2021-bulletin	0-QUA-SD_6- 200921/3537
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	08-Sep-21	10	Possible buffer overflow due to improper validation of device types during P2P search in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile,	https://www. qualcomm.co m/company/ product- security/bull etins/august- 2021-bulletin	0-QUA-SD_6- 200921/3538

1-2

0-1

4-5

5-6

6-7

7-8

8-9

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking		
			CVE ID : CVE-2021-1972		
sd_675_firmv	ware			I	
Exposure of Resource to Wrong Sphere	08-Sep-21	2.1	Child process can leak information from parent process due to numeric pids are getting compared and these pid can be reused in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wearables CVE ID : CVE-2021-1904	https://www. qualcomm.co m/company/ product- security/bull etins/august- 2021-bulletin	0-QUA-SD_6- 200921/3539
Loop with Unreachable Exit Condition ('Infinite Loop')	08-Sep-21	5	Loop with unreachable exit condition may occur due to improper handling of unsupported input in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Voice & Music, Snapdragon Wearables CVE ID : CVE-2021-1914	https://www. qualcomm.co m/company/ product- security/bull etins/august- 2021-bulletin	0-QUA-SD_6- 200921/3540
Out-of- bounds Write	08-Sep-21	10	Possible buffer underflow due to lack of check for negative indices values when processing user provided	https://www. qualcomm.co m/company/ product-	O-QUA-SD_6- 200921/3541
CVSS Scoring Sc	ale 0-1	1-2	2-3 3-4 4-5 5-6	6-7 7-8	8-9 9-10

Page 1353 of 1474

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			input in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Voice & Music, Snapdragon Wearables	security/bull etins/august- 2021-bulletin	
Integer Underflow (Wrap or Wraparoun d)	08-Sep-21	10	CVE ID : CVE-2021-1916 Integer underflow can occur when the RTCP length is lesser than than the actual blocks present in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Voice & Music, Snapdragon Wearables CVE ID : CVE-2021-1919	https://www. qualcomm.co m/company/ product- security/bull etins/august- 2021-bulletin	0-QUA-SD_6- 200921/3542
Integer Underflow (Wrap or Wraparoun d)	08-Sep-21	10	Integer underflow can occur due to improper handling of incoming RTCP packets in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Voice & Music, Snapdragon Wearables CVE ID : CVE-2021-1920	https://www. qualcomm.co m/company/ product- security/bull etins/august- 2021-bulletin	0-QUA-SD_6- 200921/3543
Incorrect Type Conversion or Cast	08-Sep-21	4.6	Incorrect pointer argument passed to trusted application TA could result in un- intended memory operations in Snapdragon Auto,	https://www. qualcomm.co m/company/ product- security/bull	0-QUA-SD_6- 200921/3544

CVSS Scoring Scale	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10
			Pa	ge 1354	of 1474					

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Snapdragon Compute, Snapdragon Connectivity, Snapdragon Industrial IOT CVE ID : CVE-2021-1923	etins/august- 2021-bulletin	
Exposure of Resource to Wrong Sphere	08-Sep-21	2.1	Lack of strict validation of bootmode can lead to information disclosure in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wearables	https://www. qualcomm.co m/company/ product- security/bull etins/august- 2021-bulletin	O-QUA-SD_6- 200921/3545
Improper Restriction of Operations within the Bounds of a Memory Buffer	08-Sep-21	3.6	CVE ID : CVE-2021-1929 Possible out of bounds read due to incorrect validation of incoming buffer length in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile CVE ID : CVE-2021-1930	https://www. qualcomm.co m/company/ product- security/bull etins/august- 2021-bulletin	0-QUA-SD_6- 200921/3546
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	08-Sep-21	10	Possible buffer overflow due to improper validation of device types during P2P search in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Woice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and	https://www. qualcomm.co m/company/ product- security/bull etins/august- 2021-bulletin	0-QUA-SD_6- 200921/3547

0-1

1-2

7-8

5-6

6-7

8-9

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Networking		
			CVE ID : CVE-2021-1972		
sd_8cx_firmw	are				
Exposure of Resource to Wrong Sphere	08-Sep-21	2.1	Child process can leak information from parent process due to numeric pids are getting compared and these pid can be reused in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wearables CVE ID : CVE-2021-1904	https://www. qualcomm.co m/company/ product- security/bull etins/august- 2021-bulletin	0-QUA-SD_8- 200921/3548
Loop with Unreachable Exit Condition ('Infinite Loop')	08-Sep-21	5	Loop with unreachable exit condition may occur due to improper handling of unsupported input in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Voice & Music, Snapdragon Wearables CVE ID : CVE-2021-1914	https://www. qualcomm.co m/company/ product- security/bull etins/august- 2021-bulletin	0-QUA-SD_8- 200921/3549
Out-of- bounds Write	08-Sep-21	10	Possible buffer underflow due to lack of check for negative indices values when processing user provided input in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT,	https://www. qualcomm.co m/company/ product- security/bull etins/august- 2021-bulletin	0-QUA-SD_8- 200921/3550
CVSS Scoring Sc	ale 0-1	1-2	2-3 3-4 4-5 5-6	6-7 7-8	8-9 9-10

Page 1356 of 1474

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Voice & Music, Snapdragon Wearables		
			CVE ID : CVE-2021-1916		
Integer Underflow (Wrap or Wraparoun d)	08-Sep-21	10	Integer underflow can occur when the RTCP length is lesser than than the actual blocks present in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Voice & Music, Snapdragon Wearables CVE ID : CVE-2021-1919	https://www. qualcomm.co m/company/ product- security/bull etins/august- 2021-bulletin	0-QUA-SD_8- 200921/3551
Integer Underflow (Wrap or Wraparoun d)	08-Sep-21	10	Integer underflow can occur due to improper handling of incoming RTCP packets in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Voice & Music, Snapdragon Wearables CVE ID : CVE-2021-1920	https://www. qualcomm.co m/company/ product- security/bull etins/august- 2021-bulletin	0-QUA-SD_8- 200921/3552
Incorrect Type Conversion or Cast	08-Sep-21	4.6	Incorrect pointer argument passed to trusted application TA could result in un- intended memory operations in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Industrial IOT CVE ID : CVE-2021-1923	https://www. qualcomm.co m/company/ product- security/bull etins/august- 2021-bulletin	0-QUA-SD_8- 200921/3553
CVSS Scoring Sc	ale 0-1	1-2	2-3 3-4 4-5 5-6 Page 1357 of 1474	6-7 7-8	8-9 9-10

Page 1357 of 1474

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	08-Sep-21	10	Possible buffer overflow due to improper validation of device types during P2P search in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wired Infrastructure and Networking CVE ID : CVE-2021-1972	https://www. qualcomm.co m/company/ product- security/bull etins/august- 2021-bulletin	0-QUA-SD_8- 200921/3554
sd_8c_firmwa	are				
Exposure of Resource to Wrong Sphere	08-Sep-21	2.1	Child process can leak information from parent process due to numeric pids are getting compared and these pid can be reused in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wearables CVE ID : CVE-2021-1904	https://www. qualcomm.co m/company/ product- security/bull etins/august- 2021-bulletin	0-QUA-SD_8- 200921/3555
Loop with Unreachable Exit Condition ('Infinite Loop')	08-Sep-21	5	Loop with unreachable exit condition may occur due to improper handling of unsupported input in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT,	https://www. qualcomm.co m/company/ product- security/bull etins/august- 2021-bulletin	0-QUA-SD_8- 200921/3556

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Snapdragon IoT, Snapdragon Voice & Music, Snapdragon Wearables CVE ID : CVE-2021-1914		
Out-of- bounds Write	08-Sep-21	10	Possible buffer underflow due to lack of check for negative indices values when processing user provided input in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Voice & Music, Snapdragon Wearables CVE ID : CVE-2021-1916	https://www. qualcomm.co m/company/ product- security/bull etins/august- 2021-bulletin	O-QUA-SD_8- 200921/3557
Integer Underflow (Wrap or Wraparoun d)	08-Sep-21	10	Integer underflow can occur when the RTCP length is lesser than than the actual blocks present in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Voice & Music, Snapdragon Wearables CVE ID : CVE-2021-1919	https://www. qualcomm.co m/company/ product- security/bull etins/august- 2021-bulletin	O-QUA-SD_8- 200921/3558
Integer Underflow (Wrap or Wraparoun d)	08-Sep-21	10	Integer underflow can occur due to improper handling of incoming RTCP packets in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon	https://www. qualcomm.co m/company/ product- security/bull etins/august- 2021-bulletin	0-QUA-SD_8- 200921/3559

0-1

1-2

2-3 3-4

4-5

5-6

6-7

7-8

8-9

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Voice & Music, Snapdragon Wearables CVE ID : CVE-2021-1920		
Incorrect Type Conversion or Cast	08-Sep-21	4.6	Incorrect pointer argument passed to trusted application TA could result in un- intended memory operations in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Industrial IOT CVE ID : CVE-2021-1923	https://www. qualcomm.co m/company/ product- security/bull etins/august- 2021-bulletin	0-QUA-SD_8- 200921/3560
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	08-Sep-21	10	Possible buffer overflow due to improper validation of device types during P2P search in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Woice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking CVE ID : CVE-2021-1972	https://www. qualcomm.co m/company/ product- security/bull etins/august- 2021-bulletin	0-QUA-SD_8- 200921/3561
sm4125_firm	iware				
Exposure of Resource to Wrong Sphere	08-Sep-21	2.1	Child process can leak information from parent process due to numeric pids are getting compared and these pid can be reused in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT,	https://www. qualcomm.co m/company/ product- security/bull etins/august- 2021-bulletin	O-QUA-SM41- 200921/3562
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 & CVE ID	Patch	NCIIPC ID
			Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables CVE ID : CVE-2021-1904		
			Incorrect pointer argument		
Incorrect Type Conversion or Cast	08-Sep-21	4.6	passed to trusted application TA could result in un- intended memory operations in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Industrial IOT CVE ID : CVE-2021-1923	https://www. qualcomm.co m/company/ product- security/bull etins/august- 2021-bulletin	0-QUA-SM41- 200921/3563
Improper Restriction of Operations within the Bounds of a Memory Buffer	08-Sep-21	3.6	Possible out of bounds read due to incorrect validation of incoming buffer length in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile	https://www. qualcomm.co m/company/ product- security/bull etins/august- 2021-bulletin	0-QUA-SM41- 200921/3564
			CVE ID : CVE-2021-1930		
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	08-Sep-21	10	Possible buffer overflow due to improper validation of device types during P2P search in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Woice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking CVE ID : CVE-2021-1972	https://www. qualcomm.co m/company/ product- security/bull etins/august- 2021-bulletin	0-QUA-SM41- 200921/3565
CVSS Scoring Sca	ale 0-1	1-2	2-3 3-4 4-5 5-6	6-7 7-8	8-9 9-10

Page 1361 of 1474

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
sm6250p_fir	mware				
Exposure of Resource to Wrong Sphere	08-Sep-21	2.1	Child process can leak information from parent process due to numeric pids are getting compared and these pid can be reused in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wearables CVE ID : CVE-2021-1904	https://www. qualcomm.co m/company/ product- security/bull etins/august- 2021-bulletin	0-QUA-SM62- 200921/3566
Loop with Unreachable Exit Condition ('Infinite Loop')	08-Sep-21	5	Loop with unreachable exit condition may occur due to improper handling of unsupported input in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Voice & Music, Snapdragon Wearables CVE ID : CVE-2021-1914	https://www. qualcomm.co m/company/ product- security/bull etins/august- 2021-bulletin	0-QUA-SM62- 200921/3567
Out-of- bounds Write	08-Sep-21	10	Possible buffer underflow due to lack of check for negative indices values when processing user provided input in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Voice & Music, Snapdragon	https://www. qualcomm.co m/company/ product- security/bull etins/august- 2021-bulletin	0-QUA-SM62- 200921/3568

Page 1362 of 1474

Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
		Wearables		
		CVE ID : CVE-2021-1916		
08-Sep-21	10	when the RTCP length islesser than than the actualblocks present in SnapdragonAuto, Snapdragon Compute,Snapdragon Connectivity,Snapdragon Consumer IOT,Snapdragon Industrial IOT,Snapdragon IoT, SnapdragonVoice & Music, SnapdragonWearables		0-QUA-SM62- 200921/3569
08-Sep-21	10	Integer underflow can occur due to improper handling of incoming RTCP packets in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Voice & Music, Snapdragon Wearables CVE ID : CVE-2021-1920	https://www. qualcomm.co m/company/ product- security/bull etins/august- 2021-bulletin	0-QUA-SM62- 200921/3570
08-Sep-21	3.6	Possible out of bounds read due to incorrect validation of incoming buffer length in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile CVE ID : CVE-2021-1930	https://www. qualcomm.co m/company/ product- security/bull etins/august- 2021-bulletin	0-QUA-SM62- 200921/3571
08-Sep-21	10	Possible buffer overflow due to improper validation of	https://www. qualcomm.co	0-QUA-SM62- 8-9 9-10
	08-Sep-21 08-Sep-21	08-Sep-21 10 08-Sep-21 10 08-Sep-21 3.6 08-Sep-21 10	Image: constraint of the series of the ser	Image: Note of the image of

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID	
Checking Size of Input ('Classic Buffer Overflow')			device types during P2P search in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Woice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking CVE ID : CVE-2021-1972	m/company/ product- security/bull etins/august- 2021-bulletin	200921/3572	
sm6250_firm	iware					
Exposure of Resource to Wrong Sphere	08-Sep-21	2.1	Child process can leak information from parent process due to numeric pids are getting compared and these pid can be reused in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables CVE ID : CVE-2021-1904	https://www. qualcomm.co m/company/ product- security/bull etins/august- 2021-bulletin	0-QUA-SM62- 200921/3573	
Loop with Unreachable Exit Condition ('Infinite Loop')		Loop with unreachable exit condition may occur due to improper handling of unsupported input in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Voice & Music, Snapdragon	https://www. qualcomm.co m/company/ product- security/bull etins/august- 2021-bulletin	0-QUA-SM62- 200921/3574		

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Wearables		
			CVE ID : CVE-2021-1914		
Out-of- bounds Write	08-Sep-21	10	Possible buffer underflow due to lack of check for negative indices values when processing user provided input in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, 		O-QUA-SM62- 200921/3575
			CVE ID : CVE-2021-1916		
Integer Underflow (Wrap or Wraparoun d)	08-Sep-21	10	Integer underflow can occur when the RTCP length is lesser than than the actual blocks present in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Voice & Music, Snapdragon Wearables CVE ID : CVE-2021-1919	https://www. qualcomm.co m/company/ product- security/bull etins/august- 2021-bulletin	0-QUA-SM62- 200921/3576
Integer Underflow (Wrap or Wraparoun d)	08-Sep-21	10	Integer underflow can occur due to improper handling of incoming RTCP packets in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Voice & Music, Snapdragon Wearables	https://www. qualcomm.co m/company/ product- security/bull etins/august- 2021-bulletin	0-QUA-SM62- 200921/3577
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 & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2021-1920		
Incorrect Type Conversion or Cast	08-Sep-21	4.6	Incorrect pointer argument passed to trusted application TA could result in un- intended memory operations in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Industrial IOT CVE ID : CVE-2021-1923	https://www. qualcomm.co m/company/ product- security/bull etins/august- 2021-bulletin	0-QUA-SM62- 200921/3578
Exposure of Resource to Wrong Sphere	08-Sep-21	2.1	Lack of strict validation of bootmode can lead to information disclosure in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wearables CVE ID : CVE-2021-1929	https://www. qualcomm.co m/company/ product- security/bull etins/august- 2021-bulletin	0-QUA-SM62- 200921/3579
Improper Restriction of Operations within the Bounds of a Memory Buffer	08-Sep-21	3.6	CVE ID : CVE-2021-1929Possible out of bounds read due to incorrect validation of incoming buffer length in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobilehttps://www qualcomm.co m/company/ product- security/bull etins/august- 2021-bulletimCVE ID : CVE-2021-1930https://www qualcomm.co		0-QUA-SM62- 200921/3580
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	08-Sep-21	10	Possible buffer overflow due to improper validation of device types during P2P search in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT,	https://www. qualcomm.co m/company/ product- security/bull etins/august- 2021-bulletin	0-QUA-SM62- 200921/3581

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking		
			CVE ID : CVE-2021-1972		
sm7250_firm	iware			1	1
Exposure of Resource to Wrong Sphere	08-Sep-21	2.1	Child process can leak information from parent process due to numeric pids are getting compared and these pid can be reused in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wearables CVE ID : CVE-2021-1904	https://www. qualcomm.co m/company/ product- security/bull etins/august- 2021-bulletin	0-QUA-SM72- 200921/3582
Loop with Unreachable Exit Condition ('Infinite Loop')	08-Sep-21	5	Loop with unreachable exit condition may occur due to improper handling of unsupported input in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Voice & Music, Snapdragon Wearables CVE ID : CVE-2021-1914	https://www. qualcomm.co m/company/ product- security/bull etins/august- 2021-bulletin	0-QUA-SM72- 200921/3583
Out-of- bounds	08-Sep-21	10	Possible buffer underflow due to lack of check for	https://www. qualcomm.co	0-QUA-SM72- 200921/3584
		10 1-2			200921/3584 8-9 9-10

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Write			negative indices values when processing user provided input in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Voice & Music, Snapdragon Wearables CVE ID : CVE-2021-1916	m/company/ product- security/bull etins/august- 2021-bulletin	
Integer Underflow (Wrap or Wraparoun d)	08-Sep-21	10	Integer underflow can occur when the RTCP length is lesser than than the actual blocks present in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Voice & Music, Snapdragon Wearables CVE ID : CVE-2021-1919	https://www. qualcomm.co m/company/ product- security/bull etins/august- 2021-bulletin	0-QUA-SM72- 200921/3585
Integer Underflow (Wrap or Wraparoun d)	08-Sep-21	10	Integer underflow can occur due to improper handling of incoming RTCP packets in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Voice & Music, Snapdragon Wearables	https://www. qualcomm.co m/company/ product- security/bull etins/august- 2021-bulletin	0-QUA-SM72- 200921/3586
Incorrect			CVE ID : CVE-2021-1920 Incorrect pointer argument	https://www.	0-QUA-SM72-
Type Conversion	08-Sep-21	4.6	passed to trusted application TA could result in un-	qualcomm.co m/company/	200921/3587

CVSS Scoring Scale	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10
Page 1368 of 1474										

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
or Cast			intended memory operations in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Industrial IOT CVE ID : CVE-2021-1923	product- security/bull etins/august- 2021-bulletin	
Exposure of Resource to Wrong Sphere	08-Sep-21	2.1	Lack of strict validation of bootmode can lead to information disclosure in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wearables CVE ID : CVE-2021-1929	https://www. qualcomm.co m/company/ product- security/bull etins/august- 2021-bulletin	O-QUA-SM72- 200921/3588
Improper Restriction of Operations within the Bounds of a Memory Buffer	08-Sep-21	3.6	Possible out of bounds read due to incorrect validation of incoming buffer length in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile CVE ID : CVE-2021-1930	https://www. qualcomm.co m/company/ product- security/bull etins/august- 2021-bulletin	0-QUA-SM72- 200921/3589
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	08-Sep-21	10	Possible buffer overflow due to improper validation of device types during P2P search in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables,	https://www. qualcomm.co m/company/ product- security/bull etins/august- 2021-bulletin	O-QUA-SM72- 200921/3590

1-2 2-3

0-1

5-6

6-7

7-8

8-9

	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Snapdragon Wired Infrastructure and Networking		
			CVE ID : CVE-2021-1972		
sm7325_firm	iware				
Exposure of Resource to Wrong Sphere	08-Sep-21	2.1	Child process can leak information from parent process due to numeric pids are getting compared and these pid can be reused in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wearables CVE ID : CVE-2021-1904	https://www. qualcomm.co m/company/ product- security/bull etins/august- 2021-bulletin	O-QUA-SM73- 200921/3591
Incorrect Type Conversion or Cast	08-Sep-21	4.6	Incorrect pointer argument passed to trusted application TA could result in un- intended memory operations in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Industrial IOT CVE ID : CVE-2021-1923	https://www. qualcomm.co m/company/ product- security/bull etins/august- 2021-bulletin	0-QUA-SM73- 200921/3592
Exposure of Resource to Wrong Sphere	08-Sep-21	2.1	Lack of strict validation of bootmode can lead to information disclosure in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wearables	https://www. qualcomm.co m/company/ product- security/bull etins/august- 2021-bulletin	0-QUA-SM73- 200921/3593

Page 1370 of 1474

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2021-1929		
Improper Restriction of Operations within the Bounds of a Memory Buffer	08-Sep-21	3.6	Possible out of bounds read due to incorrect validation of incoming buffer length in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile CVE ID : CVE-2021-1930	https://www. qualcomm.co m/company/ product- security/bull etins/august- 2021-bulletin	0-QUA-SM73- 200921/3594
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	08-Sep-21	10	Possible buffer overflow due to improper validation of device types during P2P search in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Woice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking CVE ID : CVE-2021-1972	https://www. qualcomm.co m/company/ product- security/bull etins/august- 2021-bulletin	0-QUA-SM73- 200921/3595
wcd9306_fir	mware				
Exposure of Resource to Wrong Sphere	08-Sep-21	2.1	Child process can leak information from parent process due to numeric pids are getting compared and these pid can be reused in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile,	https://www. qualcomm.co m/company/ product- security/bull etins/august- 2021-bulletin	O-QUA- WCD9- 200921/3596

CVSS Scoring Scale	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10
			Pa	age 1371	of 1474					

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Snapdragon Voice & Music, Snapdragon Wearables		
			CVE ID : CVE-2021-1904		
Loop with Unreachable Exit Condition ('Infinite Loop')	08-Sep-21	5	Loop with unreachable exit condition may occur due to improper handling of unsupported input in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Voice & Music, Snapdragon Wearables CVE ID : CVE-2021-1914	https://www. qualcomm.co m/company/ product- security/bull etins/august- 2021-bulletin	O-QUA- WCD9- 200921/3597
Out-of- bounds Write	08-Sep-21	10	Possible buffer underflow due to lack of check for negative indices values when processing user provided input in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Voice & Music, Snapdragon Wearables CVE ID : CVE-2021-1916	https://www. qualcomm.co m/company/ product- security/bull etins/august- 2021-bulletin	O-QUA- WCD9- 200921/3598
Integer Underflow (Wrap or Wraparoun d)	08-Sep-21	10	Integer underflow can occur when the RTCP length is lesser than than the actual blocks present in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon	https://www. qualcomm.co m/company/ product- security/bull etins/august- 2021-bulletin	O-QUA- WCD9- 200921/3599

0-1

1-2

2-3 3-4 4-5 Page 1372 of 1474 6-7

5-6

7-8

8-9

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Voice & Music, Snapdragon Wearables		
			CVE ID : CVE-2021-1919		
Integer Underflow (Wrap or Wraparoun d)	08-Sep-21	10	Integer underflow can occur due to improper handling of incoming RTCP packets in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Voice & Music, Snapdragon Wearables	https://www. qualcomm.co m/company/ product- security/bull etins/august- 2021-bulletin	0-QUA- WCD9- 200921/3600
			CVE ID : CVE-2021-1920		
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	08-Sep-21	10	Possible buffer overflow due to improper validation of device types during P2P search in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Woice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking CVE ID : CVE-2021-1972	https://www. qualcomm.co m/company/ product- security/bull etins/august- 2021-bulletin	O-QUA- WCD9- 200921/3601
wcd9326_firi	mware				
Exposure of Resource to Wrong Sphere	08-Sep-21	2.1	Child process can leak information from parent process due to numeric pids are getting compared and these pid can be reused in Snapdragon Auto, Snapdragon Compute,	https://www. qualcomm.co m/company/ product- security/bull etins/august- 2021-bulletin	O-QUA- WCD9- 200921/3602
CVSS Scoring Sc	ale 0-1	1-2	2-3 3-4 4-5 5-6 Page 1373 of 1474	6-7 7-8	8-9 9-10

Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
		Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables		
		CVE ID : CVE-2021-1904		
08-Sep-21	3.6	Buffer over read could occur due to incorrect check of buffer size while flashing emmc devices in Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking	https://www. qualcomm.co m/company/ product- security/bull etins/august- 2021-bulletin	0-QUA- WCD9- 200921/3603
08-Sep-21	2.1	Lack of strict validation of bootmode can lead to information disclosure in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wearables CVE ID : CVE-2021-1929	https://www. qualcomm.co m/company/ product- security/bull etins/august- 2021-bulletin	0-QUA- WCD9- 200921/3604
08-Sep-21	3.6	Possible out of bounds read due to incorrect validation of incoming buffer length in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT,	https://www. qualcomm.co m/company/ product- security/bull etins/august- 2021-bulletin	O-QUA- WCD9- 200921/3605
	08-Sep-21 08-Sep-21	08-Sep-21 3.6 08-Sep-21 2.1	Image: construct of the struct of the stru	and BarbonSnapdragon Connectivity, Snapdragon Mobile, Snapdragon Mobile, Snapdragon Wearablesand Snapdragon WearablesCVE ID: CVE-2021-1904CVE ID: CVE-2021-190408-Sep-213.6Buffer over read could occur due to incorrect check of buffer size while flashing emmc devices in Snapdragon Industrial IOT, Snapdragon Connectivity, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Mobile, Snapdragon Mobile, Snapdragon Networkinghttps://www. qualcomm.co m/company/ product- security/bull etins/august- 2021-bulletin08-Sep-212.1Lack of strict validation of bootmode can lead to information disclosure in Snapdragon Consumer IOT, Snapdragon Consumer IOT, Snapdragon Auto, Snapdragon Consumer IOT, Snapdragon Consumer IOT, Snapdragon Auto, Snapdragon Consumer IOT, Snapdragon Consumer IOT, Snapdragon Mobile, Snapdragon Wired Infrastructure and Networkinghttps://www. qualcomm.co m/company/ product- security/bull etins/august- 2021-bulletin08-Sep-212.1Eack of strict validation of bootmode can lead to information disclosure in Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Consumer IOT, Snapdragon Mobile, Snapdragon Consumer IOT, Snapdragon Mobile, Snapdragon Mobile, Snapdragon Mobile, Snapdragon Mobile, Snapdragon Mobile, Snapdragon Mobile, Snapdragon Mobile, Snapdragon Mobile, Snapdragon Consumer IOT, Snapdragon Mobile, Snapdragon M

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Buffer			Snapdragon Industrial IOT, Snapdragon Mobile CVE ID : CVE-2021-1930		
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	08-Sep-21	10	Possible buffer overflow due to improper validation of device types during P2P search in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Woice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking CVE ID : CVE-2021-1972	https://www. qualcomm.co m/company/ product- security/bull etins/august- 2021-bulletin	0-QUA- WCD9- 200921/3606
wcd9330_firi	mware				
Exposure of Resource to Wrong Sphere	08-Sep-21	2.1	Child process can leak information from parent process due to numeric pids are getting compared and these pid can be reused in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wearables CVE ID : CVE-2021-1904	https://www. qualcomm.co m/company/ product- security/bull etins/august- 2021-bulletin	O-QUA- WCD9- 200921/3607
Loop with Unreachable Exit Condition ('Infinite	08-Sep-21	5	Loop with unreachable exit condition may occur due to improper handling of unsupported input in Snapdragon Auto,	https://www. qualcomm.co m/company/ product- security/bull	O-QUA- WCD9- 200921/3608
CVSS Scoring Sc	ale 0-1	1-2	2-3 3-4 4-5 5-6	6-7 7-8	8-9 9-10

Page 1375 of 1474

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Loop')			Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Voice & Music, Snapdragon Wearables CVE ID : CVE-2021-1914	etins/august- 2021-bulletin	
Out-of- bounds Write	08-Sep-21	10	Possible buffer underflow due to lack of check for negative indices values when processing user provided input in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Voice & Music, Snapdragon Wearables CVE ID : CVE-2021-1916	https://www. qualcomm.co m/company/ product- security/bull etins/august- 2021-bulletin	O-QUA- WCD9- 200921/3609
Integer Underflow (Wrap or Wraparoun d)	08-Sep-21	10	Integer underflow can occur when the RTCP length is lesser than than the actual blocks present in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Voice & Music, Snapdragon Wearables CVE ID : CVE-2021-1919	https://www. qualcomm.co m/company/ product- security/bull etins/august- 2021-bulletin	O-QUA- WCD9- 200921/3610
Integer Underflow (Wrap or Wraparoun d)	08-Sep-21	10	Integer underflow can occur due to improper handling of incoming RTCP packets in Snapdragon Auto, Snapdragon Compute,	https://www. qualcomm.co m/company/ product- security/bull	O-QUA- WCD9- 200921/3611
CVSS Scoring Sc	ale 0-1	1-2	2-3 3-4 4-5 5-6	6-7 7-8	8-9 9-10

Page 1376 of 1474

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Voice & Music, Snapdragon Wearables	etins/august- 2021-bulletin	
			CVE ID : CVE-2021-1920		
Out-of- bounds Read	08-Sep-21	3.6	Buffer over read could occur due to incorrect check of buffer size while flashing emmc devices in Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking	https://www. qualcomm.co m/company/ product- security/bull etins/august- 2021-bulletin	0-QUA- WCD9- 200921/3612
			CVE ID : CVE-2021-1928		
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	08-Sep-21	10	Possible buffer overflow due to improper validation of device types during P2P search in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Woice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking CVE ID : CVE-2021-1972	https://www. qualcomm.co m/company/ product- security/bull etins/august- 2021-bulletin	0-QUA- WCD9- 200921/3613
wcd9335_fir	mware				
Exposure of Resource to	08-Sep-21	2.1	Child process can leak information from parent	https://www. qualcomm.co	O-QUA- WCD9-
CVSS Scoring Sc	ale 0-1	1-2	2-3 3-4 4-5 5-6 Page 1377 of 1474	6-7 7-8	8-9 9-10

Wrong SphereSphereBuffer Copy without Checking Size of Input ('Classic Buffer Overflow')08-Sep-2 08-Sep-2wcd9340_firmware		process due to numeric pids are getting compared and these pid can be reused in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wearables CVE ID : CVE-2021-1904 Possible buffer overflow due	m/company/ product- security/bull etins/august- 2021-bulletin	200921/3614
without Checking Size of Input 08-Sep-2 ('Classic Buffer Overflow')		Possible buffer overflow due		
wcd9340_firmware	21 10	to improper validation of device types during P2P search in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Woice & Music, Snapdragon Wired Infrastructure and Networking CVE ID : CVE-2021-1972	https://www. qualcomm.co m/company/ product- security/bull etins/august- 2021-bulletin	0-QUA- WCD9- 200921/3615
Exposure of Resource to Wrong Sphere	21 2 .1	Child process can leak information from parent process due to numeric pids are getting compared and these pid can be reused in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile,	https://www. qualcomm.co m/company/ product- security/bull etins/august- 2021-bulletin	0-QUA- WCD9- 200921/3616

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Snapdragon Voice & Music, Snapdragon Wearables		
			CVE ID : CVE-2021-1904		
Loop with Unreachable Exit Condition ('Infinite Loop')	08-Sep-21	5	Loop with unreachable exit condition may occur due to improper handling of unsupported input in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Voice & Music, Snapdragon Wearables CVE ID : CVE-2021-1914	https://www. qualcomm.co m/company/ product- security/bull etins/august- 2021-bulletin	O-QUA- WCD9- 200921/3617
Out-of- bounds Write	08-Sep-21	10	Possible buffer underflow due to lack of check for negative indices values when processing user provided input in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Voice & Music, Snapdragon Wearables	https://www. qualcomm.co m/company/ product- security/bull etins/august- 2021-bulletin	0-QUA- WCD9- 200921/3618
			CVE ID : CVE-2021-1916 Integer underflow can occur when the RTCP length is	https://www.	
Integer Underflow (Wrap or Wraparoun d)	08-Sep-21	10	lesser than than the actual blocks present in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon	qualcomm.co m/company/ product- security/bull etins/august- 2021-bulletin	0-QUA- WCD9- 200921/3619

0-1

1-2

2-3 3-4 4-5 Page 1379 of 1474 7-8

5-6

6-7

8-9

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Voice & Music, Snapdragon Wearables		
			CVE ID : CVE-2021-1919		
Integer Underflow (Wrap or Wraparoun d)	08-Sep-21	10	Integer underflow can occur due to improper handling of incoming RTCP packets in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Voice & Music, Snapdragon Wearables	https://www. qualcomm.co m/company/ product- security/bull etins/august- 2021-bulletin	O-QUA- WCD9- 200921/3620
			CVE ID : CVE-2021-1920		
Incorrect Type Conversion or Cast	08-Sep-21	4.6	Incorrect pointer argument passed to trusted application TA could result in un- intended memory operations in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Industrial IOT CVE ID : CVE-2021-1923	https://www. qualcomm.co m/company/ product- security/bull etins/august- 2021-bulletin	O-QUA- WCD9- 200921/3621
Out-of- bounds Read	08-Sep-21	3.6	Buffer over read could occur due to incorrect check of buffer size while flashing emmc devices in Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking CVE ID : CVE-2021-1928	https://www. qualcomm.co m/company/ product- security/bull etins/august- 2021-bulletin	O-QUA- WCD9- 200921/3622

CVSS Scoring Scale	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10
			Pa	age 1380	of 1474					

Exposure of Resource to Wrong Sphere08-Sep-21bootmode of information Snapdragor Sna	disclosure in Auto, Compute, Connectivity, Consumer IOT, Industrial IOT, Mobile,	https://www. qualcomm.co	
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')08-Sep-2110Snapdragor Snapdragor Snapdragor Snapdragor Snapdragor Snapdragor Snapdragor Snapdragor Snapdragor Snapdragor Snapdragor Snapdragor Snapdragor Snapdragor Snapdragor Snapdragor 	Wearables E-2021-1929	m/company/ product- security/bull etins/august- 2021-bulletin	0-QUA- WCD9- 200921/3623
Exposure of Esponence to Espone	Connectivity, Consumer IOT, Industrial IOT, Mobile, Voice & Music, Wearables, Wired re and	https://www. qualcomm.co m/company/ product- security/bull etins/august- 2021-bulletin	0-QUA- WCD9- 200921/3624
Exposure of these pid ca Besource to Spandrager			
Nessure to Wrong08-Sep-212.1Snapdragor SnapdragorSphereSnapdragorSnapdragorSnapdragorSnapdragorSnapdragorSnapdragorSnapdragorSnapdragorSnapdragorSnapdragorSnapdragorSnapdragor	from parent to numeric pids	https://www. qualcomm.co m/company/ product- security/bull etins/august- 2021-bulletin	0-QUA- WCD9- 200921/3625

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Snapdragon Wearables		
			CVE ID : CVE-2021-1904		
Exposure of Resource to Wrong Sphere	08-Sep-21	2.1	Lack of strict validation of bootmode can lead to information disclosure in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wearables CVE ID : CVE-2021-1929	https://www. qualcomm.co m/company/ product- security/bull etins/august- 2021-bulletin	0-QUA- WCD9- 200921/3626
Improper Restriction of Operations within the Bounds of a Memory Buffer	08-Sep-21	3.6	Possible out of bounds read due to incorrect validation of incoming buffer length in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile CVE ID : CVE-2021-1930	https://www. qualcomm.co m/company/ product- security/bull etins/august- 2021-bulletin	0-QUA- WCD9- 200921/3627
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	08-Sep-21	10	Possible buffer overflow due to improper validation of device types during P2P search in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Woice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking CVE ID : CVE-2021-1972	https://www. qualcomm.co m/company/ product- security/bull etins/august- 2021-bulletin	0-QUA- WCD9- 200921/3628
CVSS Scoring Sc	ale 0-1	1-2	2-3 3-4 4-5 5-6	6-7 7-8	8-9 9-10

Page 1382 of 1474

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
wcd9360_fir	mware				
Loop with Unreachable Exit Condition ('Infinite Loop')	08-Sep-21	5	Loop with unreachable exit condition may occur due to improper handling of unsupported input in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Voice & Music, Snapdragon Wearables CVE ID : CVE-2021-1914	https://www. qualcomm.co m/company/ product- security/bull etins/august- 2021-bulletin	O-QUA- WCD9- 200921/3629
Out-of- bounds Write	08-Sep-21	10	Possible buffer underflow due to lack of check for negative indices values when processing user provided input in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Voice & Music, Snapdragon Wearables CVE ID : CVE-2021-1916	https://www. qualcomm.co m/company/ product- security/bull etins/august- 2021-bulletin	O-QUA- WCD9- 200921/3630
Integer Underflow (Wrap or Wraparoun d)	08-Sep-21	10	Integer underflow can occur when the RTCP length is lesser than than the actual blocks present in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Voice & Music, Snapdragon Wearables	https://www. qualcomm.co m/company/ product- security/bull etins/august- 2021-bulletin	O-QUA- WCD9- 200921/3631

0-1

1-2

2-3 3-4

4-5

6-7

5-6

7-8

8-9

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2021-1919		
Integer Underflow (Wrap or Wraparoun d)	08-Sep-21	10	Integer underflow can occur due to improper handling of incoming RTCP packets in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Voice & Music, Snapdragon Wearables CVE ID : CVE-2021-1920	https://www. qualcomm.co m/company/ product- security/bull etins/august- 2021-bulletin	0-QUA- WCD9- 200921/3632
Incorrect Type Conversion or Cast	08-Sep-21	4.6	Incorrect pointer argument passed to trusted application TA could result in un- intended memory operations in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Industrial IOT CVE ID : CVE-2021-1923	https://www. qualcomm.co m/company/ product- security/bull etins/august- 2021-bulletin	0-QUA- WCD9- 200921/3633
wcd9370_fir	mware				
Exposure of Resource to Wrong Sphere	08-Sep-21	2.1	Child process can leak information from parent process due to numeric pids are getting compared and these pid can be reused in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wearables CVE ID : CVE-2021-1904	https://www. qualcomm.co m/company/ product- security/bull etins/august- 2021-bulletin	O-QUA- WCD9- 200921/3634

CVSS Scoring Scale	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10
			Pa	age 1384 (of 1474					

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Loop with Unreachable Exit Condition ('Infinite Loop')	08-Sep-21	5	Loop with unreachable exit condition may occur due to improper handling of unsupported input in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Voice & Music, Snapdragon Wearables CVE ID : CVE-2021-1914	https://www. qualcomm.co m/company/ product- security/bull etins/august- 2021-bulletin	O-QUA- WCD9- 200921/3635
Out-of- bounds Write	08-Sep-21	10	Possible buffer underflow due to lack of check for negative indices values when processing user provided input in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Voice & Music, Snapdragon Wearables CVE ID : CVE-2021-1916	https://www. qualcomm.co m/company/ product- security/bull etins/august- 2021-bulletin	O-QUA- WCD9- 200921/3636
Integer Underflow (Wrap or Wraparoun d)	08-Sep-21	10	Integer underflow can occur when the RTCP length is lesser than than the actual blocks present in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Voice & Music, Snapdragon Wearables CVE ID : CVE-2021-1919	https://www. qualcomm.co m/company/ product- security/bull etins/august- 2021-bulletin	O-QUA- WCD9- 200921/3637

1-2

5-6

6-7

7-8

8-9

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Integer Underflow (Wrap or Wraparoun d)	08-Sep-21	10	Integer underflow can occur due to improper handling of incoming RTCP packets in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Voice & Music, Snapdragon Wearables CVE ID : CVE-2021-1920	https://www. qualcomm.co m/company/ product- security/bull etins/august- 2021-bulletin	O-QUA- WCD9- 200921/3638
Incorrect Type Conversion or Cast	08-Sep-21	4.6	Incorrect pointer argument passed to trusted application TA could result in un- intended memory operations in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Industrial IOT CVE ID : CVE-2021-1923	https://www. qualcomm.co m/company/ product- security/bull etins/august- 2021-bulletin	O-QUA- WCD9- 200921/3639
Exposure of Resource to Wrong Sphere	08-Sep-21	2.1	Lack of strict validation of bootmode can lead to information disclosure in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wearables CVE ID : CVE-2021-1929	https://www. qualcomm.co m/company/ product- security/bull etins/august- 2021-bulletin	O-QUA- WCD9- 200921/3640
Improper Restriction of Operations within the Bounds of a	08-Sep-21	3.6	Possible out of bounds read due to incorrect validation of incoming buffer length in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity,	https://www. qualcomm.co m/company/ product- security/bull etins/august-	0-QUA- WCD9- 200921/3641

0-1

1-2 2-3 3-4

4-5

5-6

6-7

7-8

8-9

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Memory Buffer			Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile	2021-bulletin	
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	08-Sep-21	10	CVE ID : CVE-2021-1930 Possible buffer overflow due to improper validation of device types during P2P search in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wired Music, Snapdragon Wired Infrastructure and Networking CVE ID : CVE-2021-1972	https://www. qualcomm.co m/company/ product- security/bull etins/august- 2021-bulletin	0-QUA- WCD9- 200921/3642
wcd9371_fir	mware				
Exposure of Resource to Wrong Sphere	08-Sep-21	2.1	Child process can leak information from parent process due to numeric pids are getting compared and these pid can be reused in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wearables CVE ID : CVE-2021-1904	https://www. qualcomm.co m/company/ product- security/bull etins/august- 2021-bulletin	0-QUA- WCD9- 200921/3643
Loop with Unreachable Exit Condition	08-Sep-21	5	Loop with unreachable exit condition may occur due to improper handling of unsupported input in	https://www. qualcomm.co m/company/ product-	0-QUA- WCD9- 200921/3644
CVSS Scoring Sc	ale 0-1	1-2	2-3 3-4 4-5 5-6	6-7 7-8	8-9 9-10

Page 1387 of 1474

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
('Infinite Loop')			Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Voice & Music, Snapdragon Wearables CVE ID : CVE-2021-1914	security/bull etins/august- 2021-bulletin	
Out-of- bounds Write	08-Sep-21	10	Possible buffer underflow due to lack of check for negative indices values when processing user provided input in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Voice & Music, Snapdragon Wearables CVE ID : CVE-2021-1916	https://www. qualcomm.co m/company/ product- security/bull etins/august- 2021-bulletin	O-QUA- WCD9- 200921/3645
Integer Underflow (Wrap or Wraparoun d)	08-Sep-21	10	Integer underflow can occur when the RTCP length is lesser than than the actual blocks present in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Voice & Music, Snapdragon Wearables CVE ID : CVE-2021-1919	https://www. qualcomm.co m/company/ product- security/bull etins/august- 2021-bulletin	0-QUA- WCD9- 200921/3646
Integer Underflow (Wrap or Wraparoun	08-Sep-21	10	Integer underflow can occur due to improper handling of incoming RTCP packets in Snapdragon Auto,	https://www. qualcomm.co m/company/ product-	O-QUA- WCD9- 200921/3647

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
d)			Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Voice & Music, Snapdragon Wearables CVE ID : CVE-2021-1920	security/bull etins/august- 2021-bulletin	
Improper Restriction of Operations within the Bounds of a Memory Buffer	08-Sep-21	3.6	Possible out of bounds read due to incorrect validation of incoming buffer length in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile CVE ID : CVE-2021-1930	https://www. qualcomm.co m/company/ product- security/bull etins/august- 2021-bulletin	O-QUA- WCD9- 200921/3648
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	08-Sep-21	10	Possible buffer overflow due to improper validation of device types during P2P search in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Woice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking CVE ID : CVE-2021-1972	https://www. qualcomm.co m/company/ product- security/bull etins/august- 2021-bulletin	O-QUA- WCD9- 200921/3649
wcd9375_firi	nware				
Exposure of Resource to Wrong Sphere	08-Sep-21	2.1	Child process can leak information from parent process due to numeric pids are getting compared and	https://www. qualcomm.co m/company/ product-	O-QUA- WCD9- 200921/3650
CVSS Scoring Sc	ale 0-1	1-2	2-3 3-4 4-5 5-6 Page 1389 of 1474	6-7 7-8	8-9 9-10

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			these pid can be reused in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables CVE ID : CVE-2021-1904	security/bull etins/august- 2021-bulletin	
Loop with Unreachable Exit Condition ('Infinite Loop')	08-Sep-21	5	Loop with unreachable exit condition may occur due to improper handling of unsupported input in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Voice & Music, Snapdragon Wearables CVE ID : CVE-2021-1914	https://www. qualcomm.co m/company/ product- security/bull etins/august- 2021-bulletin	O-QUA- WCD9- 200921/3651
Out-of- bounds Write	08-Sep-21	10	Possible buffer underflow due to lack of check for negative indices values when processing user provided input in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Voice & Music, Snapdragon Wearables CVE ID : CVE-2021-1916	https://www. qualcomm.co m/company/ product- security/bull etins/august- 2021-bulletin	0-QUA- WCD9- 200921/3652
Integer Underflow	08-Sep-21	10	Integer underflow can occur when the RTCP length is	https://www. qualcomm.co	O-QUA- WCD9-

CVSS Scoring Scale	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10
Page 1390 of 1474										

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
(Wrap or Wraparoun d)			lesser than than the actual blocks present in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Voice & Music, Snapdragon Wearables CVE ID : CVE-2021-1919	m/company/ product- security/bull etins/august- 2021-bulletin	200921/3653
Integer Underflow (Wrap or Wraparoun d)	08-Sep-21	10	Integer underflow can occur due to improper handling of incoming RTCP packets in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Voice & Music, Snapdragon Wearables CVE ID : CVE-2021-1920	https://www. qualcomm.co m/company/ product- security/bull etins/august- 2021-bulletin	0-QUA- WCD9- 200921/3654
Incorrect Type Conversion or Cast	08-Sep-21	4.6	Incorrect pointer argument passed to trusted application TA could result in un- intended memory operations in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Industrial IOT CVE ID : CVE-2021-1923	https://www. qualcomm.co m/company/ product- security/bull etins/august- 2021-bulletin	0-QUA- WCD9- 200921/3655
Exposure of Resource to Wrong Sphere	08-Sep-21	2.1	Lack of strict validation of bootmode can lead to information disclosure in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT,	https://www. qualcomm.co m/company/ product- security/bull etins/august- 2021-bulletin	O-QUA- WCD9- 200921/3656
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 & CVE ID	Patch	NCIIPC ID
			Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wearables CVE ID : CVE-2021-1929		
Improper Restriction of Operations within the Bounds of a Memory Buffer	08-Sep-21	3.6	Possible out of bounds read due to incorrect validation of incoming buffer length in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile CVE ID : CVE-2021-1930	https://www. qualcomm.co m/company/ product- security/bull etins/august- 2021-bulletin	O-QUA- WCD9- 200921/3657
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	08-Sep-21	10	Possible buffer overflow due to improper validation of device types during P2P search in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Woice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking CVE ID : CVE-2021-1972	https://www. qualcomm.co m/company/ product- security/bull etins/august- 2021-bulletin	O-QUA- WCD9- 200921/3658
wcd9380_firi	mware				
Exposure of Resource to Wrong Sphere	08-Sep-21	2.1	Child process can leak information from parent process due to numeric pids are getting compared and these pid can be reused in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity,	https://www. qualcomm.co m/company/ product- security/bull etins/august- 2021-bulletin	O-QUA- WCD9- 200921/3659
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 & CVE ID	Patch	NCIIPC ID
			Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables CVE ID : CVE-2021-1904		
Loop with Unreachable Exit Condition ('Infinite Loop')	08-Sep-21	5	Loop with unreachable exit condition may occur due to improper handling of unsupported input in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Voice & Music, Snapdragon Wearables CVE ID : CVE-2021-1914	https://www. qualcomm.co m/company/ product- security/bull etins/august- 2021-bulletin	0-QUA- WCD9- 200921/3660
Out-of- bounds Write	08-Sep-21	10	Possible buffer underflow due to lack of check for negative indices values when processing user provided input in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Voice & Music, Snapdragon Wearables CVE ID : CVE-2021-1916	https://www. qualcomm.co m/company/ product- security/bull etins/august- 2021-bulletin	0-QUA- WCD9- 200921/3661
Integer Underflow (Wrap or Wraparoun d)	08-Sep-21	10	Integer underflow can occur when the RTCP length is lesser than than the actual blocks present in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity,	https://www. qualcomm.co m/company/ product- security/bull etins/august-	0-QUA- WCD9- 200921/3662

1-2

0-1

5-6

6-7

7-8

8-9

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Voice & Music, Snapdragon Wearables CVE ID : CVE-2021-1919	2021-bulletin	
Integer Underflow (Wrap or Wraparoun d)	08-Sep-21	10	Integer underflow can occur due to improper handling of incoming RTCP packets in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Voice & Music, Snapdragon Wearables CVE ID : CVE-2021-1920	https://www. qualcomm.co m/company/ product- security/bull etins/august- 2021-bulletin	0-QUA- WCD9- 200921/3663
Incorrect Type Conversion or Cast	08-Sep-21	4.6	Incorrect pointer argument passed to trusted application TA could result in un- intended memory operations in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Industrial IOT CVE ID : CVE-2021-1923	https://www. qualcomm.co m/company/ product- security/bull etins/august- 2021-bulletin	0-QUA- WCD9- 200921/3664
Exposure of Resource to Wrong Sphere	08-Sep-21	2.1	Lack of strict validation of bootmode can lead to information disclosure in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wearables CVE ID : CVE-2021-1929	https://www. qualcomm.co m/company/ product- security/bull etins/august- 2021-bulletin	O-QUA- WCD9- 200921/3665

Page 1394 of 1474

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Improper Restriction of Operations within the Bounds of a Memory Buffer	08-Sep-21	3.6	Possible out of bounds read due to incorrect validation of incoming buffer length in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile CVE ID : CVE-2021-1930	https://www. qualcomm.co m/company/ product- security/bull etins/august- 2021-bulletin	O-QUA- WCD9- 200921/3666
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	08-Sep-21	10	Possible buffer overflow due to improper validation of device types during P2P search in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Woice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking CVE ID : CVE-2021-1972	https://www. qualcomm.co m/company/ product- security/bull etins/august- 2021-bulletin	O-QUA- WCD9- 200921/3667
wcd9385_fir	mware				
Exposure of Resource to Wrong Sphere	08-Sep-21	2.1	Child process can leak information from parent process due to numeric pids are getting compared and these pid can be reused in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music,	https://www. qualcomm.co m/company/ product- security/bull etins/august- 2021-bulletin	O-QUA- WCD9- 200921/3668

CVSS Scoring Scale	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10
Page 1395 of 1474										

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Snapdragon Wearables		
			CVE ID : CVE-2021-1904		
Loop with Unreachable Exit Condition ('Infinite Loop')	08-Sep-21	5	Loop with unreachable exit condition may occur due to improper handling of unsupported input in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Voice & Music, Snapdragon Wearables CVE ID : CVE-2021-1914	https://www. qualcomm.co m/company/ product- security/bull etins/august- 2021-bulletin	0-QUA- WCD9- 200921/3669
Out-of- bounds Write	08-Sep-21	10	Possible buffer underflow due to lack of check for negative indices values when processing user provided input in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Voice & Music, Snapdragon Wearables CVE ID : CVE-2021-1916	https://www. qualcomm.co m/company/ product- security/bull etins/august- 2021-bulletin	O-QUA- WCD9- 200921/3670
Integer Underflow (Wrap or Wraparoun d)	08-Sep-21	10	Integer underflow can occur when the RTCP length is lesser than than the actual blocks present in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Voice & Music, Snapdragon	https://www. qualcomm.co m/company/ product- security/bull etins/august- 2021-bulletin	0-QUA- WCD9- 200921/3671

0-1

1-2

5-6

6-7

7-8

8-9

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Wearables		
			CVE ID : CVE-2021-1919		
Integer Underflow (Wrap or Wraparoun d)	08-Sep-21	10	Integer underflow can occur due to improper handling of incoming RTCP packets in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Voice & Music, Snapdragon Wearables CVE ID : CVE-2021-1920	https://www. qualcomm.co m/company/ product- security/bull etins/august- 2021-bulletin	0-QUA- WCD9- 200921/3672
Incorrect Type Conversion or Cast	08-Sep-21	4.6	Incorrect pointer argument passed to trusted application TA could result in un- intended memory operations in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Industrial IOT CVE ID : CVE-2021-1923	https://www. qualcomm.co m/company/ product- security/bull etins/august- 2021-bulletin	0-QUA- WCD9- 200921/3673
Exposure of Resource to Wrong Sphere	08-Sep-21	2.1	Lack of strict validation of bootmode can lead to information disclosure in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wearables CVE ID : CVE-2021-1929	https://www. qualcomm.co m/company/ product- security/bull etins/august- 2021-bulletin	0-QUA- WCD9- 200921/3674
Improper Restriction of Operations	08-Sep-21	3.6	Possible out of bounds read due to incorrect validation of incoming buffer length in Snapdragon Auto,	https://www. qualcomm.co m/company/ product-	0-QUA- WCD9- 200921/3675
CVSS Scoring Sco	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
within the Bounds of a Memory Buffer			Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile	security/bull etins/august- 2021-bulletin	
			CVE ID : CVE-2021-1930		
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	08-Sep-21	10	Possible buffer overflow due to improper validation of device types during P2P search in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Woice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking CVE ID : CVE-2021-1972	https://www. qualcomm.co m/company/ product- security/bull etins/august- 2021-bulletin	0-QUA- WCD9- 200921/3676
wcn3610_firi	mware				
Exposure of Resource to Wrong Sphere	08-Sep-21	2.1	Child process can leak information from parent process due to numeric pids are getting compared and these pid can be reused in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wearables CVE ID : CVE-2021-1904	https://www. qualcomm.co m/company/ product- security/bull etins/august- 2021-bulletin	0-QUA- WCN3- 200921/3677
		100 million (100 m			
Loop with	08-Sep-21	5	Loop with unreachable exit	https://www.	O-QUA-

3-4 4-5 5-6 Page 1398 of 1474

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Exit Condition ('Infinite Loop')			improper handling of unsupported input in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Voice & Music, Snapdragon Wearables CVE ID : CVE-2021-1914	m/company/ product- security/bull etins/august- 2021-bulletin	200921/3678
Out-of- bounds Write	08-Sep-21	10	Possible buffer underflow due to lack of check for negative indices values when processing user provided input in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Voice & Music, Snapdragon Wearables CVE ID : CVE-2021-1916	https://www. qualcomm.co m/company/ product- security/bull etins/august- 2021-bulletin	0-QUA- WCN3- 200921/3679
Integer Underflow (Wrap or Wraparoun d)	08-Sep-21	10	Integer underflow can occur when the RTCP length is lesser than than the actual blocks present in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Voice & Music, Snapdragon Wearables CVE ID : CVE-2021-1919	https://www. qualcomm.co m/company/ product- security/bull etins/august- 2021-bulletin	0-QUA- WCN3- 200921/3680
Integer Underflow	08-Sep-21	10	Integer underflow can occur due to improper handling of	https://www. qualcomm.co	O-QUA- WCN3-

CVSS Scoring Scale	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10
Page 1399 of 1474										

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
(Wrap or Wraparoun d)			incoming RTCP packets in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Voice & Music, Snapdragon Wearables CVE ID : CVE-2021-1920	m/company/ product- security/bull etins/august- 2021-bulletin	200921/3681
Out-of- bounds Read	08-Sep-21	3.6	Buffer over read could occur due to incorrect check of buffer size while flashing emmc devices in Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking CVE ID : CVE-2021-1928	https://www. qualcomm.co m/company/ product- security/bull etins/august- 2021-bulletin	0-QUA- WCN3- 200921/3682
Exposure of Resource to Wrong Sphere	08-Sep-21	2.1	Lack of strict validation of bootmode can lead to information disclosure in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wearables CVE ID : CVE-2021-1929	https://www. qualcomm.co m/company/ product- security/bull etins/august- 2021-bulletin	0-QUA- WCN3- 200921/3683
Buffer Copy without Checking Size of Input	08-Sep-21	10	Possible buffer overflow due to improper validation of device types during P2P search in Snapdragon Auto,	https://www. qualcomm.co m/company/ product-	O-QUA- WCN3- 200921/3684

CVSS Scoring Scale	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10
Page 1400 of 1474										

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
('Classic Buffer Overflow')			Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking CVE ID : CVE-2021-1972	security/bull etins/august- 2021-bulletin	
wcn3615_firm	mware				
Exposure of Resource to Wrong Sphere	08-Sep-21	2.1	Child process can leak information from parent process due to numeric pids are getting compared and these pid can be reused in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wearables CVE ID : CVE-2021-1904	https://www. qualcomm.co m/company/ product- security/bull etins/august- 2021-bulletin	0-QUA- WCN3- 200921/3685
Loop with Unreachable Exit Condition ('Infinite Loop')	08-Sep-21	5	Loop with unreachable exit condition may occur due to improper handling of unsupported input in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Voice & Music, Snapdragon Wearables	https://www. qualcomm.co m/company/ product- security/bull etins/august- 2021-bulletin	O-QUA- WCN3- 200921/3686

CVSS	Scoring	Scale
0,00	Scoring	Jeane

0-1

1-2

6-7

5-6

7-8

8-9

Write Integer Underflow	3-Sep-21	10	CVE ID : CVE-2021-1914 Possible buffer underflow due to lack of check for negative indices values when processing user provided input in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Voice & Music, Snapdragon	https://www. qualcomm.co m/company/ product- security/bull etins/august- 2021-bulletin	O-QUA- WCN3- 200921/3687
bounds 08 Write 14	3-Sep-21	10	due to lack of check for negative indices values when processing user provided input in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon	qualcomm.co m/company/ product- security/bull etins/august-	WCN3-
Underflow (Wrap or 08 Wraparoun			Wearables CVE ID : CVE-2021-1916		
	3-Sep-21	10	Integer underflow can occur when the RTCP length is lesser than than the actual blocks present in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Voice & Music, Snapdragon Wearables CVE ID : CVE-2021-1919	https://www. qualcomm.co m/company/ product- security/bull etins/august- 2021-bulletin	O-QUA- WCN3- 200921/3688
Integer Underflow (Wrap or 08 Wraparoun d)	3-Sep-21	10	Integer underflow can occur due to improper handling of incoming RTCP packets in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Voice & Music, Snapdragon Wearables	https://www. qualcomm.co m/company/ product- security/bull etins/august- 2021-bulletin	O-QUA- WCN3- 200921/3689
			CVE ID : CVE-2021-1920		
CVSS Scoring Scale		1-2	2-3 3-4 4-5 5-6 Page 1402 of 1474	6-7 7-8	8-9 9-10

SphereSnapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wearablesetins/august- 2021-bulletinBuffer Copy without Checking Size of Input (Classic Buffer08-Sep-21Possible buffer overflow due to improper validation of device types during P2P search in Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Mobile, Snapdragon Mobile, Snapdragon Onnectivity, Snapdragon Onsumer IOT, Snapdragon Vice & Music, Snapdragon Wearables, Sonapdragon Vice & Music, Snapdragon Wearables, Sonapdragon Vice & Music, Snapdragon Wearables, Sonapdragon Wearables, Sonapdragon Wearables, Sonapdragon Wearables, Sonapdragon Wearables, Sonapdragon Wired Infrastructure and Networking CVE ID: CVE-2021-1972https://www. qualcomm.co m/company/ product- security/bull etins/august- 2021-bulletin0-QUA- WCN3- 200921, etins/august- 2021-bulletinwcn3620_firtmwareChild process can leak information from parent process due to numeric pids are getting compared and these pid can be reused in Snapdragon Auto, Snapdragon Connectivity, Snapdragon Conneutivity, Snapdragon Conneutivity, Snapdragon Conneutivity, Snapdragon Conneutivity, Snapdragon Industrial IOT, Snapdragon Industrial I	PC ID	NCIIPC I	Patch	Description & CVE ID	CVSS	Publish Date	Weakness
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')08-Sep-2110to improper validation of device types during P2P search in Snapdragon Auto, Snapdragon Connectivity, Snapdragon Consumer 10T, Snapdragon Industrial I0T, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networkinghttps://www. qualcomm.co m/company/ product- security/bull etins/august- 2021-bulletinwcn3620_firmwareCVE ID : CVE-2021-1972https://www. qualcomm.co m/company/ product- security/bull etins/august- 2021-bulletinExposure of Resource to Wrong Sphere08-Sep-21AChild process can leak information from parent process due to numeric pids are getting compared and these pid can be reused in Snapdragon Connectivity, Snapdragon Connectivity, Snapdragon Connectivity, Snapdragon Connectivity, Snapdragon Consumer 10T, Snapdragon Consumer 10T, Snapdragon Connectivity, Snapdragon Consumer 10T, Snapdragon Connectivity, Snapdragon Consumer 10T, Snapdragon Consumer 10T, Snapdragon Consumer 10T, Snapdragon Connectivity, Snapdragon Consumer 10T, Snapdragon Mobile, <td>-</td> <td>-</td> <td>qualcomm.co m/company/ product- security/bull etins/august-</td> <td>bootmode can lead to information disclosure in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wearables</td> <td>2.1</td> <td>08-Sep-21</td> <td>Resource to Wrong</td>	-	-	qualcomm.co m/company/ product- security/bull etins/august-	bootmode can lead to information disclosure in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wearables	2.1	08-Sep-21	Resource to Wrong
Exposure of Resource to Wrong Sphere08-Sep-212.1Child process can leak information from parent process due to numeric pids are getting compared and these pid can be reused in Snapdragon Auto, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile,https://www. qualcomm.co m/company/ product- security/bull etins/august- 2021-bulletin	-	-	qualcomm.co m/company/ product- security/bull etins/august-	to improper validation of device types during P2P search in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Woice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking	10	08-Sep-21	without Checking Size of Input ('Classic Buffer
Exposure of Resource to Wrong Sphere08-Sep-212.1information from parent process due to numeric pids are getting compared and these pid can be reused in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile,https://www. qualcomm.co m/company/ product- 200921, etins/august- 2021-bulletin						mware	wcn3620_firi
Snapdragon Voice & Music,	-	-	qualcomm.co m/company/ product- security/bull etins/august-	information from parent process due to numeric pids are getting compared and these pid can be reused in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT,	2.1	08-Sep-21	Resource to Wrong

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Snapdragon Wearables		
			CVE ID : CVE-2021-1904		
Loop with Unreachable Exit Condition ('Infinite Loop')	08-Sep-21	5	Loop with unreachable exit condition may occur due to improper handling of unsupported input in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Voice & Music, Snapdragon Wearables	https://www. qualcomm.co m/company/ product- security/bull etins/august- 2021-bulletin	0-QUA- WCN3- 200921/3693
			CVE ID : CVE-2021-1914		
Out-of- bounds Write	08-Sep-21	10	Possible buffer underflow due to lack of check for negative indices values when processing user provided input in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Voice & Music, Snapdragon Wearables	https://www. qualcomm.co m/company/ product- security/bull etins/august- 2021-bulletin	0-QUA- WCN3- 200921/3694
			CVE ID : CVE-2021-1916		
Integer Underflow (Wrap or Wraparoun d)	08-Sep-21	10	Integer underflow can occur when the RTCP length is lesser than than the actual blocks present in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Voice & Music, Snapdragon	https://www. qualcomm.co m/company/ product- security/bull etins/august- 2021-bulletin	O-QUA- WCN3- 200921/3695

0-1

1-2

5-6

6-7

7-8

8-9

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Wearables		
			CVE ID : CVE-2021-1919		
Integer Underflow (Wrap or Wraparoun d)	08-Sep-21	10	Integer underflow can occur due to improper handling of incoming RTCP packets in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Voice & Music, Snapdragon Wearables CVE ID : CVE-2021-1920	https://www. qualcomm.co m/company/ product- security/bull etins/august- 2021-bulletin	O-QUA- WCN3- 200921/3696
Out-of- bounds Read	08-Sep-21	3.6	Buffer over read could occur due to incorrect check of buffer size while flashing emmc devices in Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking CVE ID : CVE-2021-1928	https://www. qualcomm.co m/company/ product- security/bull etins/august- 2021-bulletin	O-QUA- WCN3- 200921/3697
Exposure of Resource to Wrong Sphere	08-Sep-21	2.1	Lack of strict validation of bootmode can lead to information disclosure in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wearables CVE ID : CVE-2021-1929	https://www. qualcomm.co m/company/ product- security/bull etins/august- 2021-bulletin	O-QUA- WCN3- 200921/3698

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	08-Sep-21	10	Possible buffer overflow due to improper validation of device types during P2P search in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Woice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking CVE ID : CVE-2021-1972	https://www. qualcomm.co m/company/ product- security/bull etins/august- 2021-bulletin	0-QUA- WCN3- 200921/3699
wcn3660b_fi	rmware				
Exposure of Resource to Wrong Sphere	08-Sep-21	2.1	Child process can leak information from parent process due to numeric pids are getting compared and these pid can be reused in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wearables CVE ID : CVE-2021-1904	https://www. qualcomm.co m/company/ product- security/bull etins/august- 2021-bulletin	O-QUA- WCN3- 200921/3700
Loop with Unreachable Exit Condition ('Infinite Loop')	08-Sep-21	5	Loop with unreachable exit condition may occur due to improper handling of unsupported input in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT,	https://www. qualcomm.co m/company/ product- security/bull etins/august- 2021-bulletin	0-QUA- WCN3- 200921/3701

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Snapdragon IoT, Snapdragon Voice & Music, Snapdragon Wearables		
			CVE ID : CVE-2021-1914		
Out-of- bounds Write	08-Sep-21	10	Possible buffer underflow due to lack of check for negative indices values when processing user provided input in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Voice & Music, Snapdragon Wearables	https://www. qualcomm.co m/company/ product- security/bull etins/august- 2021-bulletin	O-QUA- WCN3- 200921/3702
			CVE ID : CVE-2021-1916		
Integer Underflow (Wrap or Wraparoun d)	08-Sep-21	10	Integer underflow can occur when the RTCP length is lesser than than the actual blocks present in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Voice & Music, Snapdragon Wearables	https://www. qualcomm.co m/company/ product- security/bull etins/august- 2021-bulletin	O-QUA- WCN3- 200921/3703
			CVE ID : CVE-2021-1919		
Integer Underflow (Wrap or Wraparoun d)	08-Sep-21	10	Integer underflow can occur due to improper handling of incoming RTCP packets in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon	https://www. qualcomm.co m/company/ product- security/bull etins/august- 2021-bulletin	0-QUA- WCN3- 200921/3704

1-2

0-1

5-6

6-7

7-8

8-9

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Voice & Music, Snapdragon Wearables		
			CVE ID : CVE-2021-1920		
Out-of- bounds Read	08-Sep-21	3.6	Buffer over read could occur due to incorrect check of buffer size while flashing emmc devices in Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking CVE ID : CVE-2021-1928	https://www. qualcomm.co m/company/ product- security/bull etins/august- 2021-bulletin	O-QUA- WCN3- 200921/3705
Exposure of Resource to Wrong Sphere	08-Sep-21	2.1	Lack of strict validation of bootmode can lead to information disclosure in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wearables CVE ID : CVE-2021-1929	https://www. qualcomm.co m/company/ product- security/bull etins/august- 2021-bulletin	0-QUA- WCN3- 200921/3706
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	08-Sep-21	10	Possible buffer overflow due to improper validation of device types during P2P search in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables,	https://www. qualcomm.co m/company/ product- security/bull etins/august- 2021-bulletin	O-QUA- WCN3- 200921/3707

0-1

1-2 2-3 3-4

4-5

5-6

6-7

7-8

8-9

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Snapdragon Wired Infrastructure and Networking		
			CVE ID : CVE-2021-1972		
wcn3660_fir	mware				
Exposure of Resource to Wrong Sphere	08-Sep-21	2.1	Child process can leak information from parent process due to numeric pids are getting compared and these pid can be reused in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wearables CVE ID : CVE-2021-1904	https://www. qualcomm.co m/company/ product- security/bull etins/august- 2021-bulletin	O-QUA- WCN3- 200921/3708
Loop with Unreachable Exit Condition ('Infinite Loop')	08-Sep-21	5	Loop with unreachable exit condition may occur due to improper handling of unsupported input in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Voice & Music, Snapdragon Wearables CVE ID : CVE-2021-1914	https://www. qualcomm.co m/company/ product- security/bull etins/august- 2021-bulletin	O-QUA- WCN3- 200921/3709
Out-of- bounds Write	08-Sep-21	10	Possible buffer underflow due to lack of check for negative indices values when processing user provided input in Snapdragon Auto, Snapdragon Compute,	https://www. qualcomm.co m/company/ product- security/bull etins/august-	O-QUA- WCN3- 200921/3710
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 & CVE ID	Patch	NCIIPC ID
			Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Voice & Music, Snapdragon Wearables	2021-bulletin	
			CVE ID : CVE-2021-1916		
Integer Underflow (Wrap or Wraparoun d)	08-Sep-21	10	Integer underflow can occur when the RTCP length is lesser than than the actual blocks present in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Voice & Music, Snapdragon Wearables	https://www. qualcomm.co m/company/ product- security/bull etins/august- 2021-bulletin	O-QUA- WCN3- 200921/3711
			CVE ID : CVE-2021-1919		
Integer Underflow (Wrap or Wraparoun d)	08-Sep-21	10	Integer underflow can occur due to improper handling of incoming RTCP packets in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Voice & Music, Snapdragon Wearables CVE ID : CVE-2021-1920	https://www. qualcomm.co m/company/ product- security/bull etins/august- 2021-bulletin	O-QUA- WCN3- 200921/3712
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	08-Sep-21	10	Possible buffer overflow due to improper validation of device types during P2P search in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT,	https://www. qualcomm.co m/company/ product- security/bull etins/august- 2021-bulletin	O-QUA- WCN3- 200921/3713
CVSS Scoring Sco	ale 0-1	1-2	2-3 3-4 4-5 5-6	6-7 7-8	8-9 9-10

 3-4
 4-5

 Page 1410 of 1474

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking		
			CVE ID : CVE-2021-1972		
wcn3680b_fi	rmware			1	
Exposure of Resource to Wrong Sphere	08-Sep-21	2.1	Child process can leak information from parent process due to numeric pids are getting compared and these pid can be reused in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wearables CVE ID : CVE-2021-1904	https://www. qualcomm.co m/company/ product- security/bull etins/august- 2021-bulletin	0-QUA- WCN3- 200921/3714
Loop with Unreachable Exit Condition ('Infinite Loop')	08-Sep-21	5	Loop with unreachable exit condition may occur due to improper handling of unsupported input in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Voice & Music, Snapdragon Wearables CVE ID : CVE-2021-1914	https://www. qualcomm.co m/company/ product- security/bull etins/august- 2021-bulletin	O-QUA- WCN3- 200921/3715
Out-of- bounds	08-Sep-21	10	Possible buffer underflow due to lack of check for	https://www. qualcomm.co	O-QUA- WCN3-
bounds CVSS Scoring Sc	-	1-2	due to lack of check for 2-3 3-4 4-5 5-6	qualcomm.co 6-7 7-8	WCN3- 8-9 9-10

 3-4
 4-5
 5-6

 Page 1411 of 1474

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Write			negative indices values when processing user provided input in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Voice & Music, Snapdragon Wearables CVE ID : CVE-2021-1916	m/company/ product- security/bull etins/august- 2021-bulletin	200921/3716
Integer Underflow (Wrap or Wraparoun d)	08-Sep-21	10	Integer underflow can occur when the RTCP length is lesser than than the actual blocks present in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Voice & Music, Snapdragon Wearables CVE ID : CVE-2021-1919	https://www. qualcomm.co m/company/ product- security/bull etins/august- 2021-bulletin	0-QUA- WCN3- 200921/3717
Integer Underflow (Wrap or Wraparoun d)	08-Sep-21	10	Integer underflow can occur due to improper handling of incoming RTCP packets in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Voice & Music, Snapdragon Wearables CVE ID : CVE-2021-1920	https://www. qualcomm.co m/company/ product- security/bull etins/august- 2021-bulletin	0-QUA- WCN3- 200921/3718
Out-of- bounds Read	08-Sep-21	3.6	Buffer over read could occur due to incorrect check of buffer size while flashing	https://www. qualcomm.co m/company/	0-QUA- WCN3- 200921/3719
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
			emmc devices in Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking CVE ID : CVE-2021-1928	product- security/bull etins/august- 2021-bulletin	
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	08-Sep-21	10	Possible buffer overflow due to improper validation of device types during P2P search in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Woice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking CVE ID : CVE-2021-1972	https://www. qualcomm.co m/company/ product- security/bull etins/august- 2021-bulletin	O-QUA- WCN3- 200921/3720
wcn3680_fir	mware				
Exposure of Resource to Wrong Sphere	08-Sep-21	2.1	Child process can leak information from parent process due to numeric pids are getting compared and these pid can be reused in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music,	https://www. qualcomm.co m/company/ product- security/bull etins/august- 2021-bulletin	0-QUA- WCN3- 200921/3721

CVSS Scoring Scale	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10
			Ра	ge 1413 (of 1474					

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Snapdragon Wearables		
			CVE ID : CVE-2021-1904		
Loop with Unreachable Exit Condition ('Infinite Loop')	08-Sep-21	5	Loop with unreachable exit condition may occur due to improper handling of unsupported input in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Voice & Music, Snapdragon Wearables	https://www. qualcomm.co m/company/ product- security/bull etins/august- 2021-bulletin	0-QUA- WCN3- 200921/3722
			CVE ID : CVE-2021-1914		
Out-of- bounds Write	08-Sep-21	10	Possible buffer underflow due to lack of check for negative indices values when processing user provided input in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Voice & Music, Snapdragon Wearables	https://www. qualcomm.co m/company/ product- security/bull etins/august- 2021-bulletin	0-QUA- WCN3- 200921/3723
			CVE ID : CVE-2021-1916		
Integer Underflow (Wrap or Wraparoun d)	08-Sep-21	10	Integer underflow can occur when the RTCP length is lesser than than the actual blocks present in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Voice & Music, Snapdragon	https://www. qualcomm.co m/company/ product- security/bull etins/august- 2021-bulletin	O-QUA- WCN3- 200921/3724

0-1

1-2

2-3 3-4 4-5 Page 1414 of 1474 5-6

6-7

7-8

8-9

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Wearables		
			CVE ID : CVE-2021-1919		
Integer Underflow (Wrap or Wraparoun d)	08-Sep-21	10	Integer underflow can occur due to improper handling of incoming RTCP packets in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Voice & Music, Snapdragon Wearables	https://www. qualcomm.co m/company/ product- security/bull etins/august- 2021-bulletin	O-QUA- WCN3- 200921/3725
			CVE ID : CVE-2021-1920		
Exposure of Resource to Wrong Sphere	08-Sep-21	2.1	Lack of strict validation of bootmode can lead to information disclosure in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wearables CVE ID : CVE-2021-1929	https://www. qualcomm.co m/company/ product- security/bull etins/august- 2021-bulletin	O-QUA- WCN3- 200921/3726
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	08-Sep-21	10	Possible buffer overflow due to improper validation of device types during P2P search in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Woice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and	https://www. qualcomm.co m/company/ product- security/bull etins/august- 2021-bulletin	0-QUA- WCN3- 200921/3727

0-1

1-2

7-8

5-6

6-7

8-9

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Networking		
			CVE ID : CVE-2021-1972		
wcn3910_firi	nware				
Exposure of Resource to Wrong Sphere	08-Sep-21	2.1	Child process can leak information from parent process due to numeric pids are getting compared and these pid can be reused in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wearables CVE ID : CVE-2021-1904	https://www. qualcomm.co m/company/ product- security/bull etins/august- 2021-bulletin	0-QUA- WCN3- 200921/3728
Loop with Unreachable Exit Condition ('Infinite Loop')	08-Sep-21	5	Loop with unreachable exit condition may occur due to improper handling of unsupported input in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Voice & Music, Snapdragon Wearables CVE ID : CVE-2021-1914	https://www. qualcomm.co m/company/ product- security/bull etins/august- 2021-bulletin	0-QUA- WCN3- 200921/3729
Out-of- bounds Write	08-Sep-21	10	Possible buffer underflow due to lack of check for negative indices values when processing user provided input in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT,	https://www. qualcomm.co m/company/ product- security/bull etins/august- 2021-bulletin	O-QUA- WCN3- 200921/3730
CVSS Scoring Sc	ale 0-1	1-2	2-3 3-4 4-5 5-6	6-7 7-8	8-9 9-10

Page 1416 of 1474

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Voice & Music, Snapdragon Wearables		
			CVE ID : CVE-2021-1916		
Integer Underflow (Wrap or Wraparoun d)	08-Sep-21	10	Integer underflow can occur when the RTCP length is lesser than than the actual blocks present in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Voice & Music, Snapdragon Wearables CVE ID : CVE-2021-1919	https://www. qualcomm.co m/company/ product- security/bull etins/august- 2021-bulletin	0-QUA- WCN3- 200921/3731
Integer Underflow (Wrap or Wraparoun d)	08-Sep-21	10	Integer underflow can occur due to improper handling of incoming RTCP packets in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Voice & Music, Snapdragon Wearables CVE ID : CVE-2021-1920	https://www. qualcomm.co m/company/ product- security/bull etins/august- 2021-bulletin	O-QUA- WCN3- 200921/3732
			Incorrect pointer argument		
Incorrect Type Conversion or Cast	08-Sep-21	4.6	passed to trusted application TA could result in un- intended memory operations in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Industrial IOT CVE ID : CVE-2021-1923	https://www. qualcomm.co m/company/ product- security/bull etins/august- 2021-bulletin	0-QUA- WCN3- 200921/3733
CVSS Scoring Sc	ale 0-1	1-2	2-3 3-4 4-5 5-6 Page 1417 of 1474	6-7 7-8	8-9 9-10

Wrong Sphere Improper Restriction of Operations)8-Sep-21)8-Sep-21	2.1	Lack of strict validation of bootmode can lead to information disclosure in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wearables CVE ID : CVE-2021-1929 Possible out of bounds read due to incorrect validation of	https://www. qualcomm.co m/company/ product- security/bull etins/august- 2021-bulletin	O-QUA- WCN3- 200921/3734
Restriction of Operations within the Bounds of a Memory)8-Sep-21		due to incorrect validation of		
		3.6	incoming buffer length in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile CVE ID : CVE-2021-1930	https://www. qualcomm.co m/company/ product- security/bull etins/august- 2021-bulletin	O-QUA- WCN3- 200921/3735
Buffer Copy without Checking Size of Input 03 ('Classic Buffer Overflow'))8-Sep-21	10	Possible buffer overflow due to improper validation of device types during P2P search in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Woice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking CVE ID : CVE-2021-1972	https://www. qualcomm.co m/company/ product- security/bull etins/august- 2021-bulletin	0-QUA- WCN3- 200921/3736
wcn3950_firmv	ware				
Exposure of 0)8-Sep-21	2.1	Child process can leak	https://www.	O-QUA-

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Resource to Wrong Sphere			information from parent process due to numeric pids are getting compared and these pid can be reused in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wearables CVE ID : CVE-2021-1904	qualcomm.co m/company/ product- security/bull etins/august- 2021-bulletin	WCN3- 200921/3737
Loop with Unreachable Exit Condition ('Infinite Loop')	08-Sep-21	5	Loop with unreachable exit condition may occur due to improper handling of unsupported input in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Voice & Music, Snapdragon Wearables CVE ID : CVE-2021-1914	https://www. qualcomm.co m/company/ product- security/bull etins/august- 2021-bulletin	0-QUA- WCN3- 200921/3738
Out-of- bounds Write	08-Sep-21	10	Possible buffer underflow due to lack of check for negative indices values when processing user provided input in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Voice & Music, Snapdragon Wearables	https://www. qualcomm.co m/company/ product- security/bull etins/august- 2021-bulletin	O-QUA- WCN3- 200921/3739

CVSS Scoring Scale	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10
Page 1419 of 1474										

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2021-1916		
Integer Underflow (Wrap or Wraparoun d)	08-Sep-21	10	Integer underflow can occur when the RTCP length is lesser than than the actual blocks present in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Voice & Music, Snapdragon Wearables CVE ID : CVE-2021-1919	https://www. qualcomm.co m/company/ product- security/bull etins/august- 2021-bulletin	O-QUA- WCN3- 200921/3740
			Integer underflow can occur due to improper handling of incoming RTCP packets in	https://www.	
Integer Underflow (Wrap or Wraparoun d)	08-Sep-21	10	Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Voice & Music, Snapdragon Wearables	https://www. qualcomm.co m/company/ product- security/bull etins/august- 2021-bulletin	O-QUA- WCN3- 200921/3741
			CVE ID : CVE-2021-1920		
Incorrect Type Conversion or Cast	08-Sep-21	4.6	Incorrect pointer argument passed to trusted application TA could result in un- intended memory operations in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Industrial IOT CVE ID : CVE-2021-1923	https://www. qualcomm.co m/company/ product- security/bull etins/august- 2021-bulletin	O-QUA- WCN3- 200921/3742
Exposure of Resource to Wrong Sphere	08-Sep-21	2.1	Lack of strict validation of bootmode can lead to information disclosure in Snapdragon Auto,	https://www. qualcomm.co m/company/ product-	O-QUA- WCN3- 200921/3743
CVSS Scoring Sc	ale 0-1	1-2	2-3 3-4 4-5 5-6	6-7 7-8	8-9 9-10

Page 1420 of 1474

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wearables	security/bull etins/august- 2021-bulletin	
			CVE ID : CVE-2021-1929		
Improper Restriction of Operations within the Bounds of a Memory Buffer	08-Sep-21	3.6	Possible out of bounds read due to incorrect validation of incoming buffer length in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile CVE ID : CVE-2021-1930	https://www. qualcomm.co m/company/ product- security/bull etins/august- 2021-bulletin	O-QUA- WCN3- 200921/3744
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	08-Sep-21	10	Possible buffer overflow due to improper validation of device types during P2P search in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Woice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking CVE ID : CVE-2021-1972	https://www. qualcomm.co m/company/ product- security/bull etins/august- 2021-bulletin	0-QUA- WCN3- 200921/3745
wcn3980_firi	nware				
Exposure of Resource to Wrong Sphere	08-Sep-21	2.1	Child process can leak information from parent process due to numeric pids are getting compared and these pid can be reused in	https://www. qualcomm.co m/company/ product- security/bull	O-QUA- WCN3- 200921/3746
CVSS Scoring Sc	ale 0-1	1-2	2-3 3-4 4-5 5-6 Page 1421 of 1474	6-7 7-8	8-9 9-10

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables CVE ID : CVE-2021-1904	etins/august- 2021-bulletin	
Out-of- bounds Read	08-Sep-21	3.6	Buffer over read could occur due to incorrect check of buffer size while flashing emmc devices in Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking CVE ID : CVE-2021-1928	https://www. qualcomm.co m/company/ product- security/bull etins/august- 2021-bulletin	0-QUA- WCN3- 200921/3747
Exposure of Resource to Wrong Sphere	08-Sep-21	2.1	Lack of strict validation of bootmode can lead to information disclosure in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wearables CVE ID : CVE-2021-1929	https://www. qualcomm.co m/company/ product- security/bull etins/august- 2021-bulletin	0-QUA- WCN3- 200921/3748
Improper Restriction of Operations within the	08-Sep-21	3.6	Possible out of bounds read due to incorrect validation of incoming buffer length in Snapdragon Auto, Snapdragon Compute,	https://www. qualcomm.co m/company/ product- security/bull	O-QUA- WCN3- 200921/3749

1-2

0-1

5-6

6-7

7-8

8-9

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Bounds of a Memory Buffer			Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile	etins/august- 2021-bulletin	
			CVE ID : CVE-2021-1930		
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	08-Sep-21	10	Possible buffer overflow due to improper validation of device types during P2P search in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Woice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking CVE ID : CVE-2021-1972	https://www. qualcomm.co m/company/ product- security/bull etins/august- 2021-bulletin	0-QUA- WCN3- 200921/3750
wcn3988_firi	nware				
Exposure of Resource to Wrong Sphere	08-Sep-21	2.1	Child process can leak information from parent process due to numeric pids are getting compared and these pid can be reused in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables CVE ID : CVE-2021-1904	https://www. qualcomm.co m/company/ product- security/bull etins/august- 2021-bulletin	0-QUA- WCN3- 200921/3751
Loop with Unreachable Exit	08-Sep-21	5	Loop with unreachable exit condition may occur due to improper handling of	https://www. qualcomm.co m/company/	0-QUA- WCN3- 200921/3752

Page 1423 of 1474

Weakness	Publish Date	CVSS	Description a	& CVE ID	Pat	ch	NCII	PC ID
Condition ('Infinite Loop')			unsupported inp Snapdragon Auto Snapdragon Com Snapdragon Com Snapdragon Com Snapdragon Indu Snapdragon IoT, Voice & Music, Sn Wearables CVE ID : CVE-20	o, ipute, nectivity, sumer IOT, istrial IOT, Snapdragon napdragon	product security etins/au 2021-b	/bull ugust-		
Out-of- bounds Write	08-Sep-21	10	Possible buffer u due to lack of che negative indices processing user p input in Snapdra Snapdragon Com Snapdragon Com Snapdragon Indu Snapdragon Indu Snapdragon IoT, Voice & Music, Sn Wearables CVE ID : CVE-20	eck for values when provided gon Auto, pute, nectivity, sumer IOT, istrial IOT, Snapdragon napdragon	https:// qualcom m/com product security etins/au 2021-b	nm.co pany/ ;- 7/bull 1gust-	0-QUA WCN3- 200922	
Integer Underflow (Wrap or Wraparoun d)	08-Sep-21	10	Integer underflow when the RTCP la lesser than than blocks present in Auto, Snapdragon Snapdragon Com Snapdragon Indu Snapdragon Indu Snapdragon IoT, Voice & Music, Sn Wearables CVE ID : CVE-20	https:// qualcom m/com product security etins/au 2021-b	nm.co pany/ :- 7/bull 1gust-	0-QUA WCN3- 200922		
Integer Underflow (Wrap or	08-Sep-21	10	Integer underflor due to improper incoming RTCP p	handling of	https:// qualcon m/com	nm.co	0-QUA WCN3- 200922	
CVSS Scoring Sc	cale 0-1	1-2	2-3 3-4	4-5 5-6	6-7	7-8	8-9	9-10

Wraparoun					NCIIPC ID
d)			Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Voice & Music, Snapdragon Wearables CVE ID : CVE-2021-1920	product- security/bull etins/august- 2021-bulletin	
Incorrect Type Conversion or Cast	08-Sep-21	4.6	Incorrect pointer argument passed to trusted application TA could result in un- intended memory operations in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Industrial IOT CVE ID : CVE-2021-1923	https://www. qualcomm.co m/company/ product- security/bull etins/august- 2021-bulletin	O-QUA- WCN3- 200921/3756
Exposure of Resource to Wrong Sphere	08-Sep-21	2.1	Lack of strict validation of bootmode can lead to information disclosure in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wearables CVE ID : CVE-2021-1929	https://www. qualcomm.co m/company/ product- security/bull etins/august- 2021-bulletin	0-QUA- WCN3- 200921/3757
Improper Restriction of Operations within the Bounds of a Memory Buffer	08-Sep-21	3.6	Possible out of bounds read due to incorrect validation of incoming buffer length in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile	https://www. qualcomm.co m/company/ product- security/bull etins/august- 2021-bulletin	0-QUA- WCN3- 200921/3758

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2021-1930		
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	08-Sep-21	10	Possible buffer overflow due to improper validation of device types during P2P search in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Woice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking CVE ID : CVE-2021-1972	https://www. qualcomm.co m/company/ product- security/bull etins/august- 2021-bulletin	0-QUA- WCN3- 200921/3759
wcn3990_firi	mware				
Exposure of Resource to Wrong Sphere	08-Sep-21	2.1	Child process can leak information from parent process due to numeric pids are getting compared and these pid can be reused in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wearables CVE ID : CVE-2021-1904	https://www. qualcomm.co m/company/ product- security/bull etins/august- 2021-bulletin	0-QUA- WCN3- 200921/3760
Exposure of Resource to Wrong Sphere	08-Sep-21	2.1	Lack of strict validation of bootmode can lead to information disclosure in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT,	https://www. qualcomm.co m/company/ product- security/bull etins/august- 2021-bulletin	0-QUA- WCN3- 200921/3761
CVSS Scoring Sc	ale 0-1	1-2	2-3 3-4 4-5 5-6 Page 1426 of 1474	6-7 7-8	8-9 9-10

3-4 4-5 Page 1426 of 1474

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wearables		
			CVE ID : CVE-2021-1929		
Improper Restriction of Operations within the Bounds of a Memory Buffer	08-Sep-21	3.6	Possible out of bounds read due to incorrect validation of incoming buffer length in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile CVE ID : CVE-2021-1930	https://www. qualcomm.co m/company/ product- security/bull etins/august- 2021-bulletin	O-QUA- WCN3- 200921/3762
			Possible buffer overflow due		
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	08-Sep-21	10	Possible buffer overflow due to improper validation of device types during P2P search in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Woice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking CVE ID : CVE-2021-1972	https://www. qualcomm.co m/company/ product- security/bull etins/august- 2021-bulletin	O-QUA- WCN3- 200921/3763
wcn3991_firi	mware				
Exposure of Resource to Wrong Sphere	08-Sep-21	2.1	Child process can leak information from parent process due to numeric pids are getting compared and these pid can be reused in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity,	https://www. qualcomm.co m/company/ product- security/bull etins/august- 2021-bulletin	O-QUA- WCN3- 200921/3764
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 & CVE ID	Patch	NCIIPC ID
			Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables CVE ID : CVE-2021-1904		
Loop with Unreachable Exit Condition ('Infinite Loop')	08-Sep-21	5	Loop with unreachable exit condition may occur due to improper handling of unsupported input in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Voice & Music, Snapdragon Wearables CVE ID : CVE-2021-1914	https://www. qualcomm.co m/company/ product- security/bull etins/august- 2021-bulletin	O-QUA- WCN3- 200921/3765
Out-of- bounds Write	08-Sep-21	10	Possible buffer underflow due to lack of check for negative indices values when processing user provided input in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Voice & Music, Snapdragon Wearables CVE ID : CVE-2021-1916	https://www. qualcomm.co m/company/ product- security/bull etins/august- 2021-bulletin	O-QUA- WCN3- 200921/3766
Integer Underflow (Wrap or Wraparoun d)	08-Sep-21	10	Integer underflow can occur when the RTCP length is lesser than than the actual blocks present in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity,	https://www. qualcomm.co m/company/ product- security/bull etins/august-	O-QUA- WCN3- 200921/3767

1-2

0-1

5-6

6-7

7-8

8-9

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Voice & Music, Snapdragon Wearables CVE ID : CVE-2021-1919	2021-bulletin	
			Integer underflow can occur due to improper handling of		
Integer Underflow (Wrap or Wraparoun d)	08-Sep-21	10	incoming RTCP packets in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Voice & Music, Snapdragon Wearables	https://www. qualcomm.co m/company/ product- security/bull etins/august- 2021-bulletin	O-QUA- WCN3- 200921/3768
			CVE ID : CVE-2021-1920		
Incorrect Type Conversion or Cast	08-Sep-21	4.6	Incorrect pointer argument passed to trusted application TA could result in un- intended memory operations in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Industrial IOT CVE ID : CVE-2021-1923	https://www. qualcomm.co m/company/ product- security/bull etins/august- 2021-bulletin	O-QUA- WCN3- 200921/3769
Exposure of Resource to Wrong Sphere	08-Sep-21	2.1	Lack of strict validation of bootmode can lead to information disclosure in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wearables CVE ID : CVE-2021-1929	https://www. qualcomm.co m/company/ product- security/bull etins/august- 2021-bulletin	O-QUA- WCN3- 200921/3770

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Improper Restriction of Operations within the Bounds of a Memory Buffer	08-Sep-21	3.6	Possible out of bounds read due to incorrect validation of incoming buffer length in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile CVE ID : CVE-2021-1930	https://www. qualcomm.co m/company/ product- security/bull etins/august- 2021-bulletin	O-QUA- WCN3- 200921/3771
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	08-Sep-21	10	Possible buffer overflow due to improper validation of device types during P2P search in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Woice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking CVE ID : CVE-2021-1972	https://www. qualcomm.co m/company/ product- security/bull etins/august- 2021-bulletin	O-QUA- WCN3- 200921/3772
wcn3998_fir	mware				
Exposure of Resource to Wrong Sphere	08-Sep-21	2.1	Child process can leak information from parent process due to numeric pids are getting compared and these pid can be reused in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music,	https://www. qualcomm.co m/company/ product- security/bull etins/august- 2021-bulletin	O-QUA- WCN3- 200921/3773

CVSS Scoring Scale	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10
			Ра	ige 1430 (of 1474					

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Snapdragon Wearables		
			CVE ID : CVE-2021-1904		
Loop with Unreachable Exit Condition ('Infinite Loop')	08-Sep-21	5	Loop with unreachable exit condition may occur due to improper handling of unsupported input in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Voice & Music, Snapdragon Wearables CVE ID : CVE-2021-1914	https://www. qualcomm.co m/company/ product- security/bull etins/august- 2021-bulletin	O-QUA- WCN3- 200921/3774
Out-of- bounds Write	08-Sep-21	10	Possible buffer underflow due to lack of check for negative indices values when processing user provided input in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Voice & Music, Snapdragon Wearables CVE ID : CVE-2021-1916	https://www. qualcomm.co m/company/ product- security/bull etins/august- 2021-bulletin	O-QUA- WCN3- 200921/3775
Integer Underflow (Wrap or Wraparoun d)	08-Sep-21	10	Integer underflow can occur when the RTCP length is lesser than than the actual blocks present in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Voice & Music, Snapdragon	https://www. qualcomm.co m/company/ product- security/bull etins/august- 2021-bulletin	O-QUA- WCN3- 200921/3776

0-1

1-2

2-3 3-4 4-5 Page 1431 of 1474 7-8

5-6

6-7

8-9

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Wearables		
			CVE ID : CVE-2021-1919		
Integer Underflow (Wrap or Wraparoun d)	08-Sep-21	10	Integer underflow can occur due to improper handling of incoming RTCP packets in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Voice & Music, Snapdragon Wearables CVE ID : CVE-2021-1920	https://www. qualcomm.co m/company/ product- security/bull etins/august- 2021-bulletin	0-QUA- WCN3- 200921/3777
Incorrect Type Conversion or Cast	08-Sep-21	4.6	Incorrect pointer argument passed to trusted application TA could result in un- intended memory operations in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Industrial IOT CVE ID : CVE-2021-1923	https://www. qualcomm.co m/company/ product- security/bull etins/august- 2021-bulletin	0-QUA- WCN3- 200921/3778
Exposure of Resource to Wrong Sphere	08-Sep-21	2.1	Lack of strict validation of bootmode can lead to information disclosure in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wearables CVE ID : CVE-2021-1929	https://www. qualcomm.co m/company/ product- security/bull etins/august- 2021-bulletin	0-QUA- WCN3- 200921/3779
Improper Restriction of Operations	08-Sep-21	3.6	Possible out of bounds read due to incorrect validation of incoming buffer length in Snapdragon Auto,	https://www. qualcomm.co m/company/ product-	0-QUA- WCN3- 200921/3780
CVSS Scoring Sco	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
within the Bounds of a Memory Buffer			Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile	security/bull etins/august- 2021-bulletin	
			CVE ID : CVE-2021-1930		
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	08-Sep-21	10	Possible buffer overflow due to improper validation of device types during P2P search in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Woice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking	https://www. qualcomm.co m/company/ product- security/bull etins/august- 2021-bulletin	O-QUA- WCN3- 200921/3781
wcn3999_firi	nware		CVE ID : CVE-2021-1972		
Exposure of Resource to Wrong Sphere	08-Sep-21	2.1	Child process can leak information from parent process due to numeric pids are getting compared and these pid can be reused in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wearables CVE ID : CVE-2021-1904	https://www. qualcomm.co m/company/ product- security/bull etins/august- 2021-bulletin	O-QUA- WCN3- 200921/3782
Buffer Copy without	08-Sep-21	10	Possible buffer overflow due to improper validation of	https://www. qualcomm.co	O-QUA- WCN3-
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 & CVE ID	Patch	NCIIPC ID
Checking Size of Input ('Classic Buffer Overflow')			device types during P2P search in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Woice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking CVE ID : CVE-2021-1972	m/company/ product- security/bull etins/august- 2021-bulletin	200921/3783
wcn6740_fir	mware				
Exposure of Resource to Wrong Sphere	08-Sep-21	2.1	Child process can leak information from parent process due to numeric pids are getting compared and these pid can be reused in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables CVE ID : CVE-2021-1904	https://www. qualcomm.co m/company/ product- security/bull etins/august- 2021-bulletin	0-QUA- WCN6- 200921/3784
Out-of- bounds Write	08-Sep-21	10	Possible buffer underflow due to lack of check for negative indices values when processing user provided input in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Voice & Music, Snapdragon	https://www. qualcomm.co m/company/ product- security/bull etins/august- 2021-bulletin	0-QUA- WCN6- 200921/3785

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Wearables		
			CVE ID : CVE-2021-1916		
Incorrect Type Conversion or Cast	08-Sep-21	4.6	Incorrect pointer argument passed to trusted application TA could result in un- intended memory operations in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Industrial IOT CVE ID : CVE-2021-1923	https://www. qualcomm.co m/company/ product- security/bull etins/august- 2021-bulletin	0-QUA- WCN6- 200921/3786
Exposure of Resource to Wrong Sphere	08-Sep-21	2.1	Lack of strict validation of bootmode can lead to information disclosure in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wearables CVE ID : CVE-2021-1929	https://www. qualcomm.co m/company/ product- security/bull etins/august- 2021-bulletin	0-QUA- WCN6- 200921/3787
Improper Restriction of Operations within the Bounds of a Memory Buffer	08-Sep-21	3.6	Possible out of bounds read due to incorrect validation of incoming buffer length in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile CVE ID : CVE-2021-1930	https://www. qualcomm.co m/company/ product- security/bull etins/august- 2021-bulletin	0-QUA- WCN6- 200921/3788
Buffer Copy without Checking Size of Input ('Classic Buffer CVSS Scoring Sc	08-Sep-21 ale 0-1	10	Possible buffer overflow due to improper validation of device types during P2P search in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity,	https://www. qualcomm.co m/company/ product- security/bull etins/august-	0-QUA- WCN6- 200921/3789 8-9 9-10

Overflow')			Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile,	2021-bulletin	
			Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking CVE ID : CVE-2021-1972		
wcn6750_firmwa	are				
Exposure of Resource to Wrong Sphere	-Sep-21	2.1	Child process can leak information from parent process due to numeric pids are getting compared and these pid can be reused in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wearables CVE ID : CVE-2021-1904	https://www. qualcomm.co m/company/ product- security/bull etins/august- 2021-bulletin	O-QUA- WCN6- 200921/3790
Loop with Unreachable Exit Condition ('Infinite Loop')	-Sep-21	5	Loop with unreachable exit condition may occur due to improper handling of unsupported input in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Voice & Music, Snapdragon Wearables CVE ID : CVE-2021-1914	https://www. qualcomm.co m/company/ product- security/bull etins/august- 2021-bulletin	0-QUA- WCN6- 200921/3791
Out-of- 08-	-Sep-21	10	Possible buffer underflow	https://www.	O-QUA-

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
bounds Write			due to lack of check for negative indices values when processing user provided input in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Voice & Music, Snapdragon Wearables CVE ID : CVE-2021-1916	qualcomm.co m/company/ product- security/bull etins/august- 2021-bulletin	WCN6- 200921/3792
			Integer underflow can occur		
Integer Underflow (Wrap or Wraparoun d)	08-Sep-21	10	when the RTCP length is lesser than than the actual blocks present in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Voice & Music, Snapdragon Wearables	https://www. qualcomm.co m/company/ product- security/bull etins/august- 2021-bulletin	O-QUA- WCN6- 200921/3793
			CVE ID : CVE-2021-1919		
Integer Underflow (Wrap or Wraparoun d)	08-Sep-21	10	Integer underflow can occur due to improper handling of incoming RTCP packets in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Voice & Music, Snapdragon Wearables	https://www. qualcomm.co m/company/ product- security/bull etins/august- 2021-bulletin	0-QUA- WCN6- 200921/3794
Incorrect			CVE ID : CVE-2021-1920	https://-	0.014
Incorrect Type	08-Sep-21	4.6	Incorrect pointer argument passed to trusted application	https://www. qualcomm.co	O-QUA- WCN6-

CVSS Scoring Scale	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10
Dago 1427 of 1474										

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Conversion or Cast			TA could result in un- intended memory operations in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Industrial IOT CVE ID : CVE-2021-1923	m/company/ product- security/bull etins/august- 2021-bulletin	200921/3795
Exposure of Resource to Wrong Sphere	08-Sep-21	2.1	Lack of strict validation of bootmode can lead to information disclosure in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wearables CVE ID : CVE-2021-1929	https://www. qualcomm.co m/company/ product- security/bull etins/august- 2021-bulletin	O-QUA- WCN6- 200921/3796
Improper Restriction of Operations within the Bounds of a Memory Buffer	08-Sep-21	3.6	Possible out of bounds read due to incorrect validation of incoming buffer length in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile CVE ID : CVE-2021-1930	https://www. qualcomm.co m/company/ product- security/bull etins/august- 2021-bulletin	O-QUA- WCN6- 200921/3797
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	CopyPossible buffer overflow due to improper validation of device types during P2P search in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT		https://www. qualcomm.co m/company/ product- security/bull etins/august- 2021-bulletin	O-QUA- WCN6- 200921/3798	

0-1 1-2

5-6

6-7

7-8

8-9

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID		
			Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking				
			CVE ID : CVE-2021-1972				
wcn6850_firmware							
Exposure of Resource to Wrong Sphere	08-Sep-21	2.1	Child process can leak information from parent process due to numeric pids are getting compared and these pid can be reused in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wearables CVE ID : CVE-2021-1904	https://www. qualcomm.co m/company/ product- security/bull etins/august- 2021-bulletin	O-QUA- WCN6- 200921/3799		
Loop with Unreachable Exit Condition ('Infinite Loop')	08-Sep-21	5	Loop with unreachable exit condition may occur due to improper handling of unsupported input in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Voice & Music, Snapdragon Wearables CVE ID : CVE-2021-1914	https://www. qualcomm.co m/company/ product- security/bull etins/august- 2021-bulletin	O-QUA- WCN6- 200921/3800		
Out-of- bounds Write	08-Sep-21	10	Possible buffer underflow due to lack of check for negative indices values when processing user provided input in Snapdragon Auto,	https://www. qualcomm.co m/company/ product- security/bull	O-QUA- WCN6- 200921/3801		
CVSS Scoring Sc	ale 0-1	1-2	2-3 3-4 4-5 5-6	6-7 7-8	8-9 9-10		

Page 1439 of 1474

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID	
			Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Voice & Music, Snapdragon Wearables	etins/august- 2021-bulletin		
			CVE ID : CVE-2021-1916			
Integer Underflow (Wrap or Wraparoun d)	08-Sep-21	10	Integer underflow can occur when the RTCP length is lesser than than the actual blocks present in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Voice & Music, Snapdragon Wearables CVE ID : CVE-2021-1919	https://www. qualcomm.co m/company/ product- security/bull etins/august- 2021-bulletin	O-QUA- WCN6- 200921/3802	
Integer Underflow (Wrap or Wraparoun d)	08-Sep-21	10	Integer underflow can occur due to improper handling of incoming RTCP packets in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Voice & Music, Snapdragon Wearables CVE ID : CVE-2021-1920	https://www. qualcomm.co m/company/ product- security/bull etins/august- 2021-bulletin	O-QUA- WCN6- 200921/3803	
Incorrect Type Conversion or Cast	08-Sep-21	4.6	Incorrect pointer argument passed to trusted application TA could result in un- intended memory operations in Snapdragon Auto, Snapdragon Compute,	https://www. qualcomm.co m/company/ product- security/bull etins/august-	O-QUA- WCN6- 200921/3804	

1-2 2-3

0-1

5-6

6-7

7-8

8-9

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Snapdragon Connectivity, Snapdragon Industrial IOT CVE ID : CVE-2021-1923	2021-bulletin	
Exposure of Resource to Wrong Sphere	08-Sep-21	2.1	Lack of strict validation of bootmode can lead to information disclosure in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wearables CVE ID : CVE-2021-1929	https://www. qualcomm.co m/company/ product- security/bull etins/august- 2021-bulletin	O-QUA- WCN6- 200921/3805
Improper Restriction of Operations within the Bounds of a Memory Buffer	08-Sep-21	3.6	Possible out of bounds read due to incorrect validation of incoming buffer length in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile CVE ID : CVE-2021-1930	https://www. qualcomm.co m/company/ product- security/bull etins/august- 2021-bulletin	O-QUA- WCN6- 200921/3806
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	Infer Copy thout ecking tae of Input08-Sep-2110Possible buffer overflow due to improper validation of device types during P2P search in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music		https://www. qualcomm.co m/company/ product- security/bull etins/august- 2021-bulletin	O-QUA- WCN6- 200921/3807	
CVSS Scoring Sc	ale 0-1	1-2	2-3 3-4 4-5 5-6	6-7 7-8	8-9 9-10

 3-4
 4-5
 5-6

 Page 1441 of 1474

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2021-1972		
wcn6851_fir	mware			I	I
Exposure of Resource to Wrong Sphere	08-Sep-21	2.1	Child process can leak information from parent process due to numeric pids are getting compared and these pid can be reused in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables CVE ID : CVE-2021-1904	https://www. qualcomm.co m/company/ product- security/bull etins/august- 2021-bulletin	O-QUA- WCN6- 200921/3808
Loop with Unreachable Exit Condition ('Infinite Loop')	08-Sep-21	5	Loop with unreachable exit condition may occur due to improper handling of unsupported input in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Voice & Music, Snapdragon Wearables CVE ID : CVE-2021-1914	https://www. qualcomm.co m/company/ product- security/bull etins/august- 2021-bulletin	0-QUA- WCN6- 200921/3809
Out-of- bounds Write	08-Sep-21	10	Possible buffer underflow due to lack of check for negative indices values when processing user provided input in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT,	https://www. qualcomm.co m/company/ product- security/bull etins/august- 2021-bulletin	O-QUA- WCN6- 200921/3810

0-1

1-2

4-5

5-6

6-7

7-8

8-9

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Snapdragon IoT, Snapdragon Voice & Music, Snapdragon Wearables		
			CVE ID : CVE-2021-1916		
Integer Underflow (Wrap or Wraparoun d)	08-Sep-21	10	Integer underflow can occur when the RTCP length is lesser than than the actual blocks present in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Voice & Music, Snapdragon Wearables CVE ID : CVE-2021-1919	https://www. qualcomm.co m/company/ product- security/bull etins/august- 2021-bulletin	O-QUA- WCN6- 200921/3811
Integer Underflow (Wrap or Wraparoun d)	08-Sep-21	10	Integer underflow can occur due to improper handling of incoming RTCP packets in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Voice & Music, Snapdragon Wearables CVE ID : CVE-2021-1920	https://www. qualcomm.co m/company/ product- security/bull etins/august- 2021-bulletin	0-QUA- WCN6- 200921/3812
Incorrect Type Conversion or Cast	08-Sep-21	4.6	Incorrect pointer argument passed to trusted application TA could result in un- intended memory operations in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Industrial IOT CVE ID : CVE-2021-1923	https://www. qualcomm.co m/company/ product- security/bull etins/august- 2021-bulletin	O-QUA- WCN6- 200921/3813

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

			Lack of strict validation of		
Exposure of Resource to Wrong Sphere	08-Sep-21	2.1	bootmode can lead to information disclosure in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wearables CVE ID : CVE-2021-1929	https://www. qualcomm.co m/company/ product- security/bull etins/august- 2021-bulletin	O-QUA- WCN6- 200921/3814
Improper Restriction of Operations within the Bounds of a Memory Buffer	08-Sep-21	3.6	Possible out of bounds read due to incorrect validation of incoming buffer length in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile CVE ID : CVE-2021-1930	https://www. qualcomm.co m/company/ product- security/bull etins/august- 2021-bulletin	O-QUA- WCN6- 200921/3815
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	08-Sep-21	10	Possible buffer overflow due to improper validation of device types during P2P search in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Industrial IOT, Snapdragon Woice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking CVE ID : CVE-2021-1972	https://www. qualcomm.co m/company/ product- security/bull etins/august- 2021-bulletin	O-QUA- WCN6- 200921/3816
wcn6855_firr	nware				
	08-Sep-21	2.1	Child process can leak	https://www.	0-QUA-

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Resource to Wrong Sphere			information from parent process due to numeric pids are getting compared and these pid can be reused in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wearables CVE ID : CVE-2021-1904	qualcomm.co m/company/ product- security/bull etins/august- 2021-bulletin	WCN6- 200921/3817
Loop with Unreachable Exit Condition ('Infinite Loop')	08-Sep-21	5	Loop with unreachable exit condition may occur due to improper handling of unsupported input in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Voice & Music, Snapdragon Wearables CVE ID : CVE-2021-1914	https://www. qualcomm.co m/company/ product- security/bull etins/august- 2021-bulletin	0-QUA- WCN6- 200921/3818
Out-of- bounds Write	08-Sep-21	10	Possible buffer underflow due to lack of check for negative indices values when processing user provided input in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Voice & Music, Snapdragon Wearables	https://www. qualcomm.co m/company/ product- security/bull etins/august- 2021-bulletin	O-QUA- WCN6- 200921/3819

CVSS Scoring Scale	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10
Page 1445 of 1474										

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2021-1916		
Integer Underflow (Wrap or Wraparoun d)	08-Sep-21	10	Integer underflow can occur when the RTCP length is lesser than than the actual blocks present in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Voice & Music, Snapdragon Wearables	https://www. qualcomm.co m/company/ product- security/bull etins/august- 2021-bulletin	0-QUA- WCN6- 200921/3820
			CVE ID : CVE-2021-1919		
Integer Underflow (Wrap or Wraparoun d)	08-Sep-21	10	Integer underflow can occur due to improper handling of incoming RTCP packets in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Voice & Music, Snapdragon Wearables	https://www. qualcomm.co m/company/ product- security/bull etins/august- 2021-bulletin	0-QUA- WCN6- 200921/3821
			CVE ID : CVE-2021-1920		
Incorrect Type Conversion or Cast	08-Sep-21	4.6	Incorrect pointer argument passed to trusted application TA could result in un- intended memory operations in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Industrial IOT CVE ID : CVE-2021-1923	https://www. qualcomm.co m/company/ product- security/bull etins/august- 2021-bulletin	0-QUA- WCN6- 200921/3822
Improper Restriction of Operations	08-Sep-21	3.6	Possible out of bounds read due to incorrect validation of incoming buffer length in Snapdragon Auto,	https://www. qualcomm.co m/company/ product-	O-QUA- WCN6- 200921/3823
CVSS Scoring Sc	ale 0-1	1-2	2-3 3-4 4-5 5-6	6-7 7-8	8-9 9-10

Page 1446 of 1474

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
within the Bounds of a Memory Buffer			Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile	security/bull etins/august- 2021-bulletin	
			CVE ID : CVE-2021-1930		
wcn6856_firm	nware				
Exposure of Resource to Wrong Sphere	08-Sep-21	2.1	Child process can leak information from parent process due to numeric pids are getting compared and these pid can be reused in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables CVE ID : CVE-2021-1904	https://www. qualcomm.co m/company/ product- security/bull etins/august- 2021-bulletin	O-QUA- WCN6- 200921/3824
Loop with Unreachable Exit Condition ('Infinite Loop')	08-Sep-21	5	Loop with unreachable exit condition may occur due to improper handling of unsupported input in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Voice & Music, Snapdragon Wearables CVE ID : CVE-2021-1914	https://www. qualcomm.co m/company/ product- security/bull etins/august- 2021-bulletin	0-QUA- WCN6- 200921/3825
Out-of- bounds Write	08-Sep-21	10	Possible buffer underflow due to lack of check for negative indices values when processing user provided	https://www. qualcomm.co m/company/ product-	0-QUA- WCN6- 200921/3826
CVSS Scoring Sca	ale 0-1	1-2	2-3 3-4 4-5 5-6	6-7 7-8	8-9 9-10

Page 1447 of 1474

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			input in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Voice & Music, Snapdragon Wearables	security/bull etins/august- 2021-bulletin	
Integer Underflow (Wrap or Wraparoun d)	08-Sep-21	10	CVE ID : CVE-2021-1916 Integer underflow can occur when the RTCP length is lesser than than the actual blocks present in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Voice & Music, Snapdragon Wearables CVE ID : CVE-2021-1919	https://www. qualcomm.co m/company/ product- security/bull etins/august- 2021-bulletin	0-QUA- WCN6- 200921/3827
Integer Underflow (Wrap or Wraparoun d)	08-Sep-21	10	Integer underflow can occur due to improper handling of incoming RTCP packets in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Voice & Music, Snapdragon Wearables CVE ID : CVE-2021-1920	https://www. qualcomm.co m/company/ product- security/bull etins/august- 2021-bulletin	O-QUA- WCN6- 200921/3828
Incorrect Type Conversion or Cast	08-Sep-21	4.6	Incorrect pointer argument passed to trusted application TA could result in un- intended memory operations in Snapdragon Auto,	https://www. qualcomm.co m/company/ product- security/bull	O-QUA- WCN6- 200921/3829

[CVSS Scoring Scale	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10
				Pa	nge 1448 (of 1474					

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Snapdragon Compute, Snapdragon Connectivity, Snapdragon Industrial IOT CVE ID : CVE-2021-1923	etins/august- 2021-bulletin	
Exposure of Resource to Wrong Sphere	08-Sep-21	2.1	Lack of strict validation of bootmode can lead to information disclosure in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wearables CVE ID : CVE-2021-1929	https://www. qualcomm.co m/company/ product- security/bull etins/august- 2021-bulletin	0-QUA- WCN6- 200921/3830
Improper Restriction of Operations within the Bounds of a Memory Buffer	08-Sep-21	3.6	Possible out of bounds read due to incorrect validation of incoming buffer length in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile CVE ID : CVE-2021-1930	https://www. qualcomm.co m/company/ product- security/bull etins/august- 2021-bulletin	0-QUA- WCN6- 200921/3831
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	08-Sep-21	10	Possible buffer overflow due to improper validation of device types during P2P search in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Woice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and	https://www. qualcomm.co m/company/ product- security/bull etins/august- 2021-bulletin	O-QUA- WCN6- 200921/3832

0-1

1-2

7-8

5-6

6-7

8-9

are -Sep-21	5	Networking CVE ID : CVE-2021-1972 Loop with unreachable exit condition may occur due to improper handling of unsupported input in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Voice & Music, Snapdragon Wearables	https://www. qualcomm.co m/company/ product- security/bull etins/august- 2021-bulletin	0-QUA- WHS9- 200921/3833
	5	Loop with unreachable exit condition may occur due to improper handling of unsupported input in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Voice & Music, Snapdragon	qualcomm.co m/company/ product- security/bull etins/august-	WHS9-
	5	condition may occur due to improper handling of unsupported input in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Voice & Music, Snapdragon	qualcomm.co m/company/ product- security/bull etins/august-	WHS9-
-Sep-21	5	condition may occur due to improper handling of unsupported input in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Voice & Music, Snapdragon	qualcomm.co m/company/ product- security/bull etins/august-	WHS9-
		CVE ID : CVE-2021-1914		
-Sep-21	10	Possible buffer underflow due to lack of check for negative indices values when processing user provided input in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Voice & Music, Snapdragon Wearables CVE ID : CVE-2021-1916	https://www. qualcomm.co m/company/ product- security/bull etins/august- 2021-bulletin	0-QUA- WHS9- 200921/3834
-Sep-21	10	Integer underflow can occur when the RTCP length is lesser than than the actual blocks present in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon	https://www. qualcomm.co m/company/ product- security/bull etins/august- 2021-bulletin	0-QUA- WHS9- 200921/3835
- (Snapdragon IoT, Snapdragon Voice & Music, Snapdragon WearablesCVE ID : CVE-2021-1916Integer underflow can occur when the RTCP length is lesser than than the actual blocks present in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon	Snapdragon IoT, Snapdragon Voice & Music, Snapdragon Wearables2021-bulletinCVE ID : CVE-2021-19162021-bulletinInteger underflow can occur when the RTCP length is lesser than than the actual blocks present in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragonhttps://www. qualcomm.co m/company/ product- security/bull etins/august- 2021-bulletin

Page 1450 of 1474

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Voice & Music, Snapdragon Wearables		
			CVE ID : CVE-2021-1919		
Integer Underflow (Wrap or Wraparoun d)	08-Sep-21	10	Integer underflow can occur due to improper handling of incoming RTCP packets in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Voice & Music, Snapdragon Wearables	https://www. qualcomm.co m/company/ product- security/bull etins/august- 2021-bulletin	0-QUA- WHS9- 200921/3836
			CVE ID : CVE-2021-1920		
Incorrect Type Conversion or Cast	08-Sep-21	4.6	Incorrect pointer argument passed to trusted application TA could result in un- intended memory operations in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Industrial IOT	https://www. qualcomm.co m/company/ product- security/bull etins/august- 2021-bulletin	O-QUA- WHS9- 200921/3837
			CVE ID : CVE-2021-1923		
wsa8810_firi	nware			Γ	
Exposure of Resource to Wrong Sphere	08-Sep-21	2.1	Child process can leak information from parent process due to numeric pids are getting compared and these pid can be reused in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables	https://www. qualcomm.co m/company/ product- security/bull etins/august- 2021-bulletin	0-QUA-WSA8- 200921/3838
CVSS Scoring Sc	ale 0-1	1-2	2-3 3-4 4-5 5-6 Page 1451 of 1474	6-7 7-8	8-9 9-10

Page 1451 of 1474

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2021-1904		
Loop with Unreachable Exit Condition ('Infinite Loop')	08-Sep-21	5	Loop with unreachable exit condition may occur due to improper handling of unsupported input in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Voice & Music, Snapdragon Wearables CVE ID : CVE-2021-1914	https://www. qualcomm.co m/company/ product- security/bull etins/august- 2021-bulletin	0-QUA-WSA8- 200921/3839
Out-of- bounds Write	08-Sep-21	10	Possible buffer underflow due to lack of check for negative indices values when processing user provided input in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Voice & Music, Snapdragon Wearables CVE ID : CVE-2021-1916	https://www. qualcomm.co m/company/ product- security/bull etins/august- 2021-bulletin	0-QUA-WSA8- 200921/3840
Integer Underflow (Wrap or Wraparoun d)	08-Sep-21	10	Integer underflow can occur when the RTCP length is lesser than than the actual blocks present in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Voice & Music, Snapdragon Wearables	https://www. qualcomm.co m/company/ product- security/bull etins/august- 2021-bulletin	0-QUA-WSA8- 200921/3841

0-1

1-2

2-3 3-4

4-5

5-6

6-7

7-8

8-9

Weakness	Publish Date	CVSS	Description & CVE ID			Pat	tch	NCI	PC ID
			CVE ID : CVE-2021-1919						
Integer Underflow (Wrap or Wraparoun d)	08-Sep-21	10	Integer under due to improp incoming RTC Snapdragon A Snapdragon C Snapdragon C Snapdragon In Snapdragon In Snapdragon In Voice & Music Wearables CVE ID : CVE-	er handl P packets uto, ompute, onnectiv onsumer ndustrial oT, Snapdra	ing of s in ity, IOT, IOT, Iragon agon	https:/ qualcom m/com produc securit etins/a 2021-b	mm.co pany/ t- y/bull ugust-	-	-WSA8- 1/3842
Incorrect Type Conversion or Cast	08-Sep-21	4.6	Incorrect poin passed to trus TA could result intended mem in Snapdragon C Snapdragon C Snapdragon In CVE ID : CVE-	ted appli lt in un- nory oper n Auto, ompute, onnective ndustrial	cation rations ity, IOT	https:/ qualcon m/com produc securit etins/a 2021-b	mm.co pany/ t- y/bull ugust-	-	-WSA8- 1/3843
Out-of- bounds Read	08-Sep-21	3.6	Buffer over read could occur due to incorrect check of buffer size while flashing emmc devices in Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking CVE ID : CVE-2021-1928			https:/ qualcom m/com produc securit etins/a 2021-b	mm.co pany/ t- y/bull ugust-	-	-WSA8- 1/3844
Exposure of Resource to	08-Sep-21	2.1	Lack of strict validation of bootmode can lead to			https:/ qualcor	mm.co	-	-WSA8- 1/3845
Wrong		1 2	information d		1n 5-6	m/com	pany/	0.0	0.10
CVSS Scoring Sc	ale 0-1	1-2	2-3 3-4	4-5	0-6	0-7	7-8	8-9	9-10

Page 1453 of 1474

Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
		Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wearables CVE ID : CVE-2021-1929	product- security/bull etins/august- 2021-bulletin	
08-Sep-21	3.6	Possible out of bounds read due to incorrect validation of incoming buffer length in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile CVE ID : CVE-2021-1930	https://www. qualcomm.co m/company/ product- security/bull etins/august- 2021-bulletin	0-QUA-WSA8- 200921/3846
08-Sep-21	10	Possible buffer overflow due to improper validation of device types during P2P search in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Industrial IOT, Snapdragon Woice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking CVE ID : CVE-2021-1972	https://www. qualcomm.co m/company/ product- security/bull etins/august- 2021-bulletin	0-QUA-WSA8- 200921/3847
nware			· 	·
08-Sep-21	2.1	Child process can leak information from parent process due to numeric pids are getting compared and	https://www. qualcomm.co m/company/ product-	0-QUA-WSA8- 200921/3848
	08-Sep-21 08-Sep-21	• • • • • • • • • • • • • • • • • • •	Image: construct of the second seco	08-Sep-211Na Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer IOT, Snapdragon Mobile, Snapdragon Mobile, Snapdragon Mobile, Snapdragon Wearablesproduct- security/bull etins/august- 2021-bulletin08-Sep-2113.64Possible out of bounds read due to incorrect validation of incoming buffer length in Snapdragon Consumer IOT, Snapdragon Consumer IOT, Snapdragon Connectivity, Snapdragon Compute, Snapdragon Consumer IOT, Snapdragon Nobile, Snapdragon Nobile, Snapdragon Nobile, Snapdragon Nobile, Snapdragon Voice & Music, Snapdragon Wierd Infrastructure and Networking CVE ID : CVE-2021-1972https://www. gualcomm.co m/company/ product- security/bull etins/august- 2021-bulletin08-Sep-212.1Child process can leak information from parent process due to numeric pidshttps://www.

Page 1454 of 1474

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			these pid can be reused in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables CVE ID : CVE-2021-1904	security/bull etins/august- 2021-bulletin	
Loop with Unreachable Exit Condition ('Infinite Loop')	08-Sep-21	5	Loop with unreachable exit condition may occur due to improper handling of unsupported input in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Voice & Music, Snapdragon Wearables CVE ID : CVE-2021-1914	https://www. qualcomm.co m/company/ product- security/bull etins/august- 2021-bulletin	0-QUA-WSA8- 200921/3849
Out-of- bounds Write	08-Sep-21	10	Possible buffer underflow due to lack of check for negative indices values when processing user provided input in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Voice & Music, Snapdragon Wearables CVE ID : CVE-2021-1916	https://www. qualcomm.co m/company/ product- security/bull etins/august- 2021-bulletin	0-QUA-WSA8- 200921/3850
Integer Underflow	08-Sep-21	10	Integer underflow can occur when the RTCP length is	https://www. qualcomm.co	0-QUA-WSA8- 200921/3851
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
(Wrap or Wraparoun d)			lesser than than the actual blocks present in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Voice & Music, Snapdragon Wearables CVE ID : CVE-2021-1919	m/company/ product- security/bull etins/august- 2021-bulletin	
Integer Underflow (Wrap or Wraparoun d)	08-Sep-21	10	Integer underflow can occur due to improper handling of incoming RTCP packets in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Voice & Music, Snapdragon Wearables CVE ID : CVE-2021-1920	https://www. qualcomm.co m/company/ product- security/bull etins/august- 2021-bulletin	0-QUA-WSA8- 200921/3852
Incorrect Type Conversion or Cast	08-Sep-21	4.6	Incorrect pointer argument passed to trusted application TA could result in un- intended memory operations in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Industrial IOT CVE ID : CVE-2021-1923	https://www. qualcomm.co m/company/ product- security/bull etins/august- 2021-bulletin	0-QUA-WSA8- 200921/3853
Out-of- bounds Read	08-Sep-21	3.6	Buffer over read could occur due to incorrect check of buffer size while flashing emmc devices in Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon	https://www. qualcomm.co m/company/ product- security/bull etins/august- 2021-bulletin	0-QUA-WSA8- 200921/3854
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 & CVE ID	Patch	NCIIPC ID
			Mobile, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking CVE ID : CVE-2021-1928		
Exposure of Resource to Wrong Sphere	08-Sep-21	2.1	Lack of strict validation of bootmode can lead to information disclosure in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wearables CVE ID : CVE-2021-1929	https://www. qualcomm.co m/company/ product- security/bull etins/august- 2021-bulletin	0-QUA-WSA8- 200921/3855
Improper Restriction of Operations within the Bounds of a Memory Buffer	08-Sep-21	3.6	Possible out of bounds read due to incorrect validation of incoming buffer length in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile CVE ID : CVE-2021-1930	https://www. qualcomm.co m/company/ product- security/bull etins/august- 2021-bulletin	0-QUA-WSA8- 200921/3856
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	08-Sep-21	10	Possible buffer overflow due to improper validation of device types during P2P search in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables,	https://www. qualcomm.co m/company/ product- security/bull etins/august- 2021-bulletin	0-QUA-WSA8- 200921/3857

0-1

1-2

2-3 3-4 4-5

5-6

6-7

7-8

8-9

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Snapdragon Wired Infrastructure and Networking		
			CVE ID : CVE-2021-1972		
wsa8830_firm	nware			1	
Exposure of Resource to Wrong Sphere	08-Sep-21	2.1	Child process can leak information from parent process due to numeric pids are getting compared and these pid can be reused in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wearables CVE ID : CVE-2021-1904	https://www. qualcomm.co m/company/ product- security/bull etins/august- 2021-bulletin	0-QUA-WSA8- 200921/3858
Loop with Unreachable Exit Condition ('Infinite Loop')	08-Sep-21	5	Loop with unreachable exit condition may occur due to improper handling of unsupported input in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Voice & Music, Snapdragon Wearables CVE ID : CVE-2021-1914	https://www. qualcomm.co m/company/ product- security/bull etins/august- 2021-bulletin	0-QUA-WSA8- 200921/3859
Out-of- bounds Write	08-Sep-21	10	Possible buffer underflow due to lack of check for negative indices values when processing user provided input in Snapdragon Auto, Snapdragon Compute,	https://www. qualcomm.co m/company/ product- security/bull etins/august-	0-QUA-WSA8- 200921/3860
CVSS Scoring Sc	ale 0-1	1-2	2-3 3-4 4-5 5-6	6-7 7-8	8-9 9-10

(Wrap or Wraparoun d)08-Sep-2110Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Voice & Music, Snapdragon Wearablesproduct- security/bull etins/august- 2021-bulletin200921/38Integer Underflow (Wrap or Wraparoun d)08-Sep-21Integer underflow can occur due to improper handling of incoming RTCP packets in Snapdragon Consumer IOT, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Consumer IOT, Snapdragon Consumer IOT, Snapdragon Consumer IOT, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Voice & Music, Snapdragon V	Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Integer Underflow (Wrap or d)08-Sep-2110Integer underflow can occur when the RTCP length is lesser than than the actual blocks present in Snapdragon Auto, Snapdragon Compute, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Voice & Music, Snapdragon Wearableshttps://www. qualcomm.co m/company/ product- security/bull etins/august- 2021-bulletin0-QUA-WS 200921/38Integer Underflow (J)08-Sep-2110Integer underflow can occur Mearableshttps://www. qualcomm.co m/company/ product- security/bull etins/august- 2021-bulletin0-QUA-WS 200921/38Integer Underflow (Wrap or Wraparoun d)08-Sep-2110Integer underflow can occur due to improper handling of incoming RTCP packets in Snapdragon Consumer IOT, Snapdragon Consumer IOT, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Voice & Music, Snapdragon <br< td=""><td></td><td></td><td></td><td>Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Voice & Music, Snapdragon</td><td>2021-bulletin</td><td></td></br<>				Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Voice & Music, Snapdragon	2021-bulletin	
Integer Underflow (Wrap or Wraparoun d)08-Sep-2110when the RTCP length is lesser than than the actual blocks present in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer IOT, Snapdragon Industrial IOT, 				CVE ID : CVE-2021-1916		
Integer Underflow (Wrap or d)08-Sep-2110Integer underflow can occur due to improper handling of incoming RTCP packets in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Industrial IOT, Snapdragon INT, Snapdragon Voice & Music, Snapdragon Voice & Music, Snapdragon Unator I incorrect pointer argument passed to trusted applicationhttps://www. qualcomm.co	Underflow (Wrap or Wraparoun	08-Sep-21	10	when the RTCP length is lesser than than the actual blocks present in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Voice & Music, Snapdragon	qualcomm.co m/company/ product- security/bull etins/august-	0-QUA-WSA8- 200921/3861
Integer Underflow (Wrap or d)08-Sep-2110due to improper handling of incoming RTCP packets in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Voice & Music, Snapdragon 				CVE ID : CVE-2021-1919		
Incorrect passed to trusted application qualcomm.co	Underflow (Wrap or Wraparoun	08-Sep-21	10	due to improper handling of incoming RTCP packets in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Voice & Music, Snapdragon Wearables	qualcomm.co m/company/ product- security/bull etins/august-	0-QUA-WSA8- 200921/3862
Type 08-Sep-21 46 intended memory experience product-	Type Conversion	08-Sep-21	4.6	passed to trusted application TA could result in un- intended memory operations in Snapdragon Auto, Snapdragon Compute,	qualcomm.co m/company/ product- security/bull etins/august-	0-QUA-WSA8- 200921/3863

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Snapdragon Industrial IOT		
			CVE ID : CVE-2021-1923		
Exposure of Resource to Wrong Sphere	08-Sep-21	2.1	Lack of strict validation of bootmode can lead to information disclosure in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wearables CVE ID : CVE-2021-1929	https://www. qualcomm.co m/company/ product- security/bull etins/august- 2021-bulletin	0-QUA-WSA8- 200921/3864
Improper Restriction of Operations within the Bounds of a Memory Buffer	08-Sep-21	3.6	Possible out of bounds read due to incorrect validation of incoming buffer length in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile CVE ID : CVE-2021-1930	https://www. qualcomm.co m/company/ product- security/bull etins/august- 2021-bulletin	0-QUA-WSA8- 200921/3865
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	08-Sep-21	10	Possible buffer overflow due to improper validation of device types during P2P search in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Woice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking CVE ID : CVE-2021-1972	https://www. qualcomm.co m/company/ product- security/bull etins/august- 2021-bulletin	0-QUA-WSA8- 200921/3866
CVSS Scoring Sc	ale 0-1	1-2	2-3 3-4 4-5 5-6	6-7 7-8	8-9 9-10

Page 1460 of 1474

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
wsa8835_fir	mware	I <u> </u>		I	I
Exposure of Resource to Wrong Sphere	08-Sep-21	2.1	Child process can leak information from parent process due to numeric pids are getting compared and these pid can be reused in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wearables CVE ID : CVE-2021-1904	https://www. qualcomm.co m/company/ product- security/bull etins/august- 2021-bulletin	0-QUA-WSA8- 200921/3867
Loop with Unreachable Exit Condition ('Infinite Loop')	08-Sep-21	5	Loop with unreachable exit condition may occur due to improper handling of unsupported input in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Voice & Music, Snapdragon Wearables CVE ID : CVE-2021-1914	https://www. qualcomm.co m/company/ product- security/bull etins/august- 2021-bulletin	0-QUA-WSA8- 200921/3868
Out-of- bounds Write	08-Sep-21	10	Possible buffer underflow due to lack of check for negative indices values when processing user provided input in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Voice & Music, Snapdragon	https://www. qualcomm.co m/company/ product- security/bull etins/august- 2021-bulletin	0-QUA-WSA8- 200921/3869

Page 1461 of 1474

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Wearables		
			CVE ID : CVE-2021-1916		
Integer Underflow (Wrap or Wraparoun d)	08-Sep-21	10	Integer underflow can occur when the RTCP length is lesser than than the actual blocks present in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Voice & Music, Snapdragon Wearables	https://www. qualcomm.co m/company/ product- security/bull etins/august- 2021-bulletin	0-QUA-WSA8- 200921/3870
			CVE ID : CVE-2021-1919		
Integer Underflow (Wrap or Wraparoun d)	08-Sep-21	10	Integer underflow can occur due to improper handling of incoming RTCP packets in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Voice & Music, Snapdragon Wearables CVE ID : CVE-2021-1920	https://www. qualcomm.co m/company/ product- security/bull etins/august- 2021-bulletin	0-QUA-WSA8- 200921/3871
Incorrect Type Conversion or Cast	08-Sep-21	4.6	Incorrect pointer argument passed to trusted application TA could result in un- intended memory operations in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Industrial IOT CVE ID : CVE-2021-1923	https://www. qualcomm.co m/company/ product- security/bull etins/august- 2021-bulletin	0-QUA-WSA8- 200921/3872
Exposure of Resource to Wrong	08-Sep-21	2.1	Lack of strict validation of bootmode can lead to information disclosure in	https://www. qualcomm.co m/company/	0-QUA-WSA8- 200921/3873
CVSS Scoring Sco	ale 0-1	1-2	2-3 3-4 4-5 5-6 Page 1462 of 1474	6-7 7-8	8-9 9-10

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID				
Sphere			Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wearables CVE ID : CVE-2021-1929	product- security/bull etins/august- 2021-bulletin					
Improper Restriction of Operations within the Bounds of a Memory Buffer	08-Sep-21	3.6	Possible out of bounds read due to incorrect validation of incoming buffer length in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile CVE ID : CVE-2021-1930	https://www. qualcomm.co m/company/ product- security/bull etins/august- 2021-bulletin	0-QUA-WSA8- 200921/3874				
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	08-Sep-21	10	Possible buffer overflow due to improper validation of device types during P2P search in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Industrial IOT, Snapdragon Woice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking CVE ID : CVE-2021-1972	https://www. qualcomm.co m/company/ product- security/bull etins/august- 2021-bulletin	0-QUA-WSA8- 200921/3875				
Schneider-electric									
-	n_active_harr	nonic_	filter_firmware						
Exposure of Sensitive Information	02-Sep-21	6.5	A CWE-200: Exposure of Sensitive Information to an Unauthorized Actor	https://down load.schneide r-	O-SCH-ACCU- 200921/3876				
CVSS Scoring Sc	ale 0-1	1-2	2-3 3-4 4-5 5-6 Page 1463 of 1474	6-7 7-8	8-9 9-10				

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
to an Unauthorize d Actor			vulnerability exist in AccuSine PCS+ / PFV+ (Versions prior to V1.6.7) and AccuSine PCSn (Versions prior to V2.2.4) that could allow an authenticated attacker to access the device via FTP protocol. CVE ID : CVE-2021-22793	electric.com/f iles?p_Doc_Re f=SEVD- 2021-222-05	
accusine_pcs	p_pfvp_firmv	vare			
Exposure of Sensitive Information to an Unauthorize d Actor	02-Sep-21	6.5	A CWE-200: Exposure of Sensitive Information to an Unauthorized Actor vulnerability exist in AccuSine PCS+ / PFV+ (Versions prior to V1.6.7) and AccuSine PCSn (Versions prior to V2.2.4) that could allow an authenticated attacker to access the device via FTP protocol. CVE ID : CVE-2021-22793	https://down load.schneide r- electric.com/f iles?p_Doc_Re f=SEVD- 2021-222-05	0-SCH-ACCU- 200921/3877
silabs				I	I
iwrap					
N/A	07-Sep-21	3.3	The Bluetooth Classic implementation in Silicon Labs iWRAP 6.3.0 and earlier does not properly handle the reception of an oversized LMP packet greater than 17 bytes, allowing attackers in radio range to trigger a crash in WT32i via a crafted LMP packet. CVE ID : CVE-2021-31609	https://www. silabs.com/wi reless/blueto oth/bluegiga- classic- legacy- modules/devi ce.wt32i-a	0-SIL-IWRA- 200921/3878
ti					
cc256xcqfn-e	em_firmware				
CVSS Scoring Sc	ale 0-1	1-2	2-3 3-4 4-5 5-6 Page 1464 of 1474	6-7 7-8	8-9 9-10

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
N/A	07-Sep-21	3.3	The Bluetooth Classic implementation on the Texas Instruments CC256XCQFN- EM does not properly handle the reception of continuous LMP_AU_Rand packets, allowing attackers in radio range to trigger a denial of service (deadlock) of the device by flooding it with LMP_AU_Rand packets after the paging procedure. CVE ID : CVE-2021-34149	https://www. ti.com/produ ct/CC2564C, https://www. ti.com/tool/C C256XC-BT- SP#primary- sw	0-TI-CC25- 200921/3879
zh-jieli					
ac6901_firm	ware				
N/A	07-Sep-21	3.3	The Bluetooth Classic implementation on Zhuhai Jieli AC690X and AC692X devices does not properly handle an out-of-order LMP Setup procedure that is followed by a malformed LMP packet, allowing attackers in radio range to deadlock a device via a crafted LMP packet. The user needs to manually reboot the device to restore communication. CVE ID : CVE-2021-31611	http://www. zh- jieli.com/pro duct/68- cn.html	O-ZHAC69- 200921/3880
N/A	07-Sep-21	6.1	The Bluetooth Classic implementation on Zhuhai Jieli AC690X devices does not properly handle the reception of an oversized LMP packet greater than 17 bytes during the LMP auto rate procedure, allowing	http://www. zh- jieli.com/pro duct/68- cn.html	0-ZHAC69- 200921/3881

CVSS Scoring Scale	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-1
			Dr	ACC 1465	of 1 171					

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			attackers in radio range to trigger a deadlock via a crafted LMP packet.		
			CVE ID : CVE-2021-31612		
N/A	07-Sep-21	3.3	The Bluetooth Classic implementation on Zhuhai Jieli AC690X and AC692X devices does not properly handle the reception of a truncated LMP packet during the LMP auto rate procedure, allowing attackers in radio range to immediately crash (and restart) a device via a crafted LMP packet.	http://www. zh- jieli.com/pro duct/68- cn.html	0-ZHAC69- 200921/3882
			CVE ID : CVE-2021-31613		
ac6902_firm	ware			Γ	
N/A	07-Sep-21	6.1	The Bluetooth Classic implementation on Zhuhai Jieli AC690X devices does not properly handle the reception of an oversized LMP packet greater than 17 bytes during the LMP auto rate procedure, allowing attackers in radio range to trigger a deadlock via a crafted LMP packet. CVE ID : CVE-2021-31612	http://www. zh- jieli.com/pro duct/68- cn.html	0-ZHAC69- 200921/3883
ac6903_firm	ware				
N/A	07-Sep-21	6.1	The Bluetooth Classic implementation on Zhuhai Jieli AC690X devices does not properly handle the reception of an oversized LMP packet greater than 17 bytes during the LMP auto rate procedure, allowing	http://www. zh- jieli.com/pro duct/68- cn.html	0-ZHAC69- 200921/3884
CVSS Scoring Sc	ale 0-1	1-2	2-3 3-4 4-5 5-6 Page 1466 of 1474	6-7 7-8	8-9 9-10

Page 1466 of 1474

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			attackers in radio range to trigger a deadlock via a crafted LMP packet.		
			CVE ID : CVE-2021-31612		
ac6904_firm	ware				
N/A	07-Sep-21	6.1	The Bluetooth Classic implementation on Zhuhai Jieli AC690X devices does not properly handle the reception of an oversized LMP packet greater than 17 bytes during the LMP auto rate procedure, allowing attackers in radio range to trigger a deadlock via a crafted LMP packet.	http://www. zh- jieli.com/pro duct/68- cn.html	0-ZHAC69- 200921/3885
			CVE ID : CVE-2021-31612		
ac6905_firm	ware				
N/A	07-Sep-21	6.1	The Bluetooth Classic implementation on Zhuhai Jieli AC690X devices does not properly handle the reception of an oversized LMP packet greater than 17 bytes during the LMP auto rate procedure, allowing attackers in radio range to trigger a deadlock via a crafted LMP packet. CVE ID : CVE-2021-31612	http://www. zh- jieli.com/pro duct/68- cn.html	0-ZHAC69- 200921/3886
ac6907_firm	ware				
N/A	07-Sep-21	6.1	The Bluetooth Classic implementation on Zhuhai Jieli AC690X devices does not properly handle the reception of an oversized LMP packet greater than 17	http://www. zh- jieli.com/pro duct/68- cn.html	0-ZHAC69- 200921/3887

CVSS Scoring Scale	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10
			Pa	age 1467	of 1474					

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			bytes during the LMP auto rate procedure, allowing attackers in radio range to trigger a deadlock via a crafted LMP packet. CVE ID : CVE-2021-31612		
ac6908_firm	ware				
N/A	07-Sep-21	6.1	The Bluetooth Classic implementation on Zhuhai Jieli AC690X devices does not properly handle the reception of an oversized LMP packet greater than 17 bytes during the LMP auto rate procedure, allowing attackers in radio range to trigger a deadlock via a crafted LMP packet. CVE ID : CVE-2021-31612	http://www. zh- jieli.com/pro duct/68- cn.html	0-ZHAC69- 200921/3888
ac690n_firm	ware				
N/A	07-Sep-21	6.1	The Bluetooth Classic implementation on Zhuhai Jieli AC690X devices does not properly handle the reception of an oversized LMP packet greater than 17 bytes during the LMP auto rate procedure, allowing attackers in radio range to trigger a deadlock via a crafted LMP packet. CVE ID : CVE-2021-31612	http://www. zh- jieli.com/pro duct/68- cn.html	0-ZHAC69- 200921/3889
ac6921_firm	ware				
N/A	07-Sep-21	3.3	The Bluetooth Classic implementation on Zhuhai Jieli AC690X and AC692X devices does not properly	http://www. zh- jieli.com/pro duct/68-	0-ZHAC69- 200921/3890

CVSS Scoring Scale	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10
				age 1468	of 1474					

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			handle an out-of-order LMP Setup procedure that is followed by a malformed LMP packet, allowing attackers in radio range to deadlock a device via a crafted LMP packet. The user needs to manually reboot the device to restore communication. CVE ID : CVE-2021-31611	cn.html	
N/A	07-Sep-21	3.3	The Bluetooth Classic implementation on Zhuhai Jieli AC690X and AC692X devices does not properly handle the reception of a truncated LMP packet during the LMP auto rate procedure, allowing attackers in radio range to immediately crash (and restart) a device via a crafted LMP packet. CVE ID : CVE-2021-31613	http://www. zh- jieli.com/pro duct/68- cn.html	0-ZHAC69- 200921/3891
ac6925_firm	ware				
N/A	07-Sep-21	3.3	The Bluetooth Classic implementation on Zhuhai Jieli AC690X and AC692X devices does not properly handle an out-of-order LMP Setup procedure that is followed by a malformed LMP packet, allowing attackers in radio range to deadlock a device via a crafted LMP packet. The user needs to manually reboot the device to restore communication.	http://www. zh- jieli.com/pro duct/68- cn.html	O-ZHAC69- 200921/3892

CVSS Scoring Scale	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10
			Pa	ge 1469 (of 1474					

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2021-31611		
N/A	07-Sep-21	3.3	The Bluetooth Classic implementation on Zhuhai Jieli AC690X and AC692X devices does not properly handle the reception of a truncated LMP packet during the LMP auto rate procedure, allowing attackers in radio range to immediately crash (and restart) a device via a crafted LMP packet.	http://www. zh- jieli.com/pro duct/68- cn.html	0-ZHAC69- 200921/3893
ac6926_firm	ware		CVE ID : CVE-2021-31613		
			The Bluetooth Classic		
N/A	07-Sep-21	3.3	implementation on Zhuhai Jieli AC690X and AC692X devices does not properly handle an out-of-order LMP Setup procedure that is followed by a malformed LMP packet, allowing attackers in radio range to deadlock a device via a crafted LMP packet. The user needs to manually reboot the device to restore communication. CVE ID : CVE-2021-31611	http://www. zh- jieli.com/pro duct/68- cn.html	0-ZHAC69- 200921/3894
N/A	07-Sep-21	3.3	The Bluetooth Classic implementation on Zhuhai Jieli AC690X and AC692X devices does not properly handle the reception of a truncated LMP packet during the LMP auto rate procedure, allowing attackers in radio range to immediately crash	http://www. zh- jieli.com/pro duct/68- cn.html	0-ZHAC69- 200921/3895

5-6

6-7

1-2

7-8

8-9

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			(and restart) a device via a crafted LMP packet.		
			CVE ID : CVE-2021-31613		
ac6928_firm	wara				
aco 720_mm					
N/A	07-Sep-21	3.3	The Bluetooth Classic implementation on Zhuhai Jieli AC690X and AC692X devices does not properly handle an out-of-order LMP Setup procedure that is followed by a malformed LMP packet, allowing attackers in radio range to deadlock a device via a crafted LMP packet. The user needs to manually reboot the device to restore communication. CVE ID : CVE-2021-31611	http://www. zh- jieli.com/pro duct/68- cn.html	0-ZHAC69- 200921/3896
N/A	07-Sep-21	3.3	The Bluetooth Classic implementation on Zhuhai Jieli AC690X and AC692X devices does not properly handle the reception of a truncated LMP packet during the LMP auto rate procedure, allowing attackers in radio range to immediately crash (and restart) a device via a crafted LMP packet. CVE ID : CVE-2021-31613	http://www. zh- jieli.com/pro duct/68- cn.html	0-ZHAC69- 200921/3897
ac692n_firm	ware				
N/A	07-Sep-21	6.1	The Bluetooth Classic implementation on Zhuhai Jieli AC690X devices does not properly handle the reception of an oversized LMP packet greater than 17	http://www. zh- jieli.com/pro duct/68- cn.html	0-ZHAC69- 200921/3898
CVSS Scoring Sc	ale 0-1	1-2	2-3 3-4 4-5 5-6 Page 1471 of 1474	6-7 7-8	8-9 9-10

Page 1471 of 1474

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			bytes during the LMP auto rate procedure, allowing attackers in radio range to trigger a deadlock via a crafted LMP packet. CVE ID : CVE-2021-31612		
ac6997_firm	ware				
N/A	07-Sep-21	6.1	The Bluetooth Classic implementation on Zhuhai Jieli AC690X devices does not properly handle the reception of an oversized LMP packet greater than 17 bytes during the LMP auto rate procedure, allowing attackers in radio range to trigger a deadlock via a crafted LMP packet. CVE ID : CVE-2021-31612	http://www. zh- jieli.com/pro duct/68- cn.html	0-ZHAC69- 200921/3899
ac6998_firm	ware				
N/A	07-Sep-21	6.1	The Bluetooth Classic implementation on Zhuhai Jieli AC690X devices does not properly handle the reception of an oversized LMP packet greater than 17 bytes during the LMP auto rate procedure, allowing attackers in radio range to trigger a deadlock via a crafted LMP packet. CVE ID : CVE-2021-31612	http://www. zh- jieli.com/pro duct/68- cn.html	0-ZHAC69- 200921/3900
ac6999_firm	waro				
N/A	07-Sep-21	6.1	The Bluetooth Classic implementation on Zhuhai Jieli AC690X devices does not properly handle the	http://www. zh- jieli.com/pro duct/68-	0-ZHAC69- 200921/3901

CVSS Scoring Scale	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10
Page 1472 of 1474										

N/Aor.Sep-21A A A A Areception of an oversized LMP packet greater than 17 bytes during the LMP autor rate procedure, allowing attackers in radio range to trigger a deadlock via a crafted LMP packet. CVE ID : CVE-2021-31612cn.htmlfw-ac63_bt_sdtUCVE ID : CVE-2021-31612	Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
N/A07-Sep-21A aThe Bluetooth Classic implementation in the Zhuhai Jieli AC6366C_DEMO_V1.0 does not properly handle the reception of continuous unsolicited LMP responses, allowing attackers in radio range to trigger a denial of service (deadlock) of the device by flooding it with LMP_AU_Rand packets after paging procedure. User intervention is required to restart the device.N/A0-ZHFW-A- 200921/3902N/A07-Sep-21The Bluetooth Classic implementation in the Zhuhai Jieli AC6366C BT SDK through 0.9.1 does not properly handle the reception of truncated LMP_SC0_Link_Request packets while no other BT connections (disabling the AB5301A inquiry and page scan procedures) via aN/A0-ZHFW-A- 200921/3902				LMP packet greater than 17 bytes during the LMP auto rate procedure, allowing attackers in radio range to trigger a deadlock via a crafted LMP packet.	cn.html	
N/A07-Sep-21implementation in the Zhuhai jieli AC6366C_DEMO_V1.0 does not properly handle the reception of continuous unsolicited LMP responses, allowing attackers in radio range to trigger a denial of service (deadlock) of the device by flooding it with LMP_AU_Rand packets after paging procedure. User intervention is required to restart the device.N/A0-ZHFW-A- 200921/3902N/A0-SP-21The Bluetooth Classic implementation in the Zhuhai Jeli AC6366C DEMO_V1.0 	fw-ac63_bt_s	dk				
N/A 07-Sep-21 4.3 A 5.4 A 5.5	N/A	07-Sep-21	6.1	implementation in the Zhuhai Jieli AC6366C_DEMO_V1.0 does not properly handle the reception of continuous unsolicited LMP responses, allowing attackers in radio range to trigger a denial of service (deadlock) of the device by flooding it with LMP_AU_Rand packets after paging procedure. User intervention is required to restart the device.	N/A	
	N/A	07-Sep-21	3.3	implementation in the Zhuhai Jieli AC6366C BT SDK through 0.9.1 does not properly handle the reception of truncated LMP_SCO_Link_Request packets while no other BT connections are active, allowing attackers in radio range to prevent new BT connections (disabling the AB5301A inquiry and page scan procedures) via a	N/A	

Page 1473 of 1474

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			needs to manually perform a		
			power cycle (restart) of the		
			device to restore BT		
			connectivity.		
			CVE ID : CVE-2021-34144		

CVSS Scoring Scale	0-1	1-2	2-3	3-4	4-5	5-6	6-7	7-8	8-9	9-10	
Page 1474 of 1474											