Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Application					
30lines					
rentpress					
Improper Neutralization 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/AjaxRequests.php file which allows attackers to inject arbitrary web scripts, in versions up to and including 6.6.4. **CVE ID : CVE-2021-38323**	N/A	A-30L-RENT-170921/1
adaptivescale					
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					
addtoany_share_buttons					
Improper Neutralization 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

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Scripting')			perform Cross-Site Scripting attacks even when the unfiltered_html capability is disallowed **CVE ID : CVE-2021-24568**		
Adobe					
acrobat					
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/security/products/acrobat/apsb21-09.html	A-ADO-ACRO-170921/4
acrobat_dc					
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/security/products/acrobat/apsb21-09.html	A-ADO-ACRO-170921/5

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_reader					
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/security/products/acrobat/apsb21-09.html	A-ADO-ACRO-170921/6
acrobat_reader_dc					
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/security/products/acrobat/apsb21-09.html	A-ADO-ACRO-170921/7

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_commerce					
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/security/products/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/security/products/magento/apsb21-64.html	A-ADO-ADOB-170921/9
Improper Neutralization of Special Elements in Output Used by a Downstream 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/security/products/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 Neutralization 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/security/products/magento/apsb21-64.html	A-ADO-ADOB-170921/11
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. **CVE ID : CVE-2021-36025**	https://helpx.adobe.com/security/products/magento/apsb21-64.html	A-ADO-ADOB-170921/12
Improper Neutralization 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/security/products/magento/apsb21-64.html	A-ADO-ADOB-170921/13

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 Neutralization 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/security/products/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/security/products/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

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/products/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/security/products/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/security/products/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/security/products/magento/apsb21-64.html	A-ADO-ADOB-170921/19

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/security/products/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/security/products/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/security/products/magento/apsb21-64.html	A-ADO-ADOB-170921/22

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 Authorization	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/security/products/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/security/products/magento/apsb21-64.html	A-ADO-ADOB-170921/24
Incorrect Authorization	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/security/products/magento/apsb21-64.html	A-ADO-ADOB-170921/25

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/security/products/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/security/products/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/security/products/magento/apsb21-64.html	A-ADO-ADOB-170921/28

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/security/products/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/security/products/magento/apsb21-64.html	A-ADO-ADOB-170921/30
after_effects					
Improper Neutralization 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/ee/security/products/after_effects/apsb21-33.html	A-ADO-AFTE-170921/31

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. **CVE ID : CVE-2021-35993**	https://helpx.adobe.com/security/products/after_effects/apsb21-54.html	A-ADO-AFTE-170921/32
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/security/products/after_effects/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/security/products/after_effects/apsb21-	A-ADO-AFTE-170921/34

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/security/products/after_effects/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/security/products/after_effects/apsb21-54.html	A-ADO-AFTE-170921/36

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. **CVE ID : CVE-2021-36018**	https://helpx.adobe.com/security/products/after_effects/apsb21-54.html	A-ADO-AFTE-170921/37
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/security/products/after_effects/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/security/prod	A-ADO-BRID-170921/39

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/security/products/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/security/products/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/security/products/bridge/apsb21-	A-ADO-BRID-170921/42

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/security/products/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/security/products/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/security/products/bridge/apsb21-69.html	A-ADO-BRID-170921/45

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/security/products/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/security/products/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/security/products/bridge/apsb21-69.html	A-ADO-BRID-170921/48

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/security/products/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/security/products/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/security/products/bridge/apsb21-69.html	A-ADO-BRID-170921/51

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/security/products/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/security/products/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/security/products/bridge/apsb21-69.html	A-ADO-BRID-170921/54

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			of this issue requires user interaction in that a victim must open a malicious file. **CVE ID : CVE-2021-36079**		
captivate					
Creation of Temporary File in Directory with Insecure Permissions	01-Sep-21	4.4	Adobe Captivate version 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. **CVE ID : CVE-2021-36002**	https://helpx.adobe.com/security/products/captivate/apsb21-60.html	A-ADO-CAPT-170921/55
connect					
Violation of Secure Design Principles	01-Sep-21	4.3	Adobe 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 a Connect recording.	https://helpx.adobe.com/security/products/connect/apsb21-66.html	A-ADO-CONN-170921/56

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2021-36061		
Improper Neutralization 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/security/products/connect/apsb21-66.html	A-ADO-CONN-170921/57
Improper Neutralization 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/security/products/connect/apsb21-66.html	A-ADO-CONN-170921/58
creative_cloud					
Uncontrolled 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/security/products/creative-cloud/apsb21-31.html	A-ADO-CREA-170921/59

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			must log on to the attacker's local machine. **CVE ID : CVE-2021-28581**		
genuine_service					
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/security/products/integrity_service/apsb21-27.html	A-ADO-GENU-170921/60
illustrator					
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/security/products/illustrator/apsb21-24.html	A-ADO-ILLU-170921/61
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	https://helpx.adobe.com/security/products/illustrator/apsb21-24.html	A-ADO-ILLU-170921/62

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			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/security/products/illustrator/apsb21-24.html	A-ADO-ILLU-170921/63
magento_open_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/security/products/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/security/products/magento	A-ADO-MAGE-170921/65

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. **CVE ID : CVE-2021-36020**	/apsb21-64.html	
Improper Neutralization of Special Elements in Output Used by a Downstream 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. **CVE ID : CVE-2021-36022**	https://helpx.adobe.com/security/products/magento/apsb21-64.html	A-ADO-MAGE-170921/66
Improper Neutralization 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/security/products/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/security/products/magento/apsb21-	A-ADO-MAGE-170921/68

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. **CVE ID : CVE-2021-36025**	64.html	
Improper Neutralization 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 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/security/products/magento/apsb21-64.html	A-ADO-MAGE-170921/69
Improper Neutralization 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/security/products/magento/apsb21-64.html	A-ADO-MAGE-170921/70

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/security/products/magento/apsb21-64.html	A-ADO-MAGE-170921/71
Improper Authorization	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/security/products/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/security/products/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/security/prod	A-ADO-MAGE-170921/74

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Pathname to a Restricted Directory ('Path Traversal')			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**	ucts/magento/apsb21-64.html	
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 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**	https://helpx.adobe.com/security/products/magento/apsb21-64.html	A-ADO-MAGE-170921/75
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://helpx.adobe.com/security/products/magento/apsb21-64.html	A-ADO-MAGE-170921/76
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	https://helpx.adobe.com/security/prod	A-ADO-MAGE-170921/77

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. **CVE ID : CVE-2021-36034**	ucts/magento/apsb21-64.html	
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/security/products/magento/apsb21-64.html	A-ADO-MAGE-170921/78
Incorrect Authorization	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/security/products/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/security/products/magento/apsb21-64.html	A-ADO-MAGE-170921/80

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 Authorization	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/security/products/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/security/products/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/security/products/magento/apsb21-64.html	A-ADO-MAGE-170921/83

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. **CVE ID : CVE-2021-36042**	https://helpx.adobe.com/security/products/magento/apsb21-64.html	A-ADO-MAGE-170921/84
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/security/products/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/security/products/magento/apsb21-64.html	A-ADO-MAGE-170921/86

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2021-36044		
media_encoder					
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 must open a malicious file. **CVE ID : CVE-2021-28569**	https://helpx.adobe.com/security/products/media-encoder/apsb21-32.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/security/products/media-encoder/apsb21-70.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/security/products/medium/apsb21-34.html	A-ADO-MEDI-170921/89

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					
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/security/products/photoshop/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/security/products/photoshop/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/security/prod	A-ADO-XMP_-170921/92

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/security/products/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/security/products/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/security/products/xmpcore/apsb21-65.html	A-ADO-XMP_-170921/95

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/security/products/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/security/products/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/security/products/xmpcore/apsb21-65.html	A-ADO-XMP_-170921/98

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2021-36052		
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-2021-36053**	https://helpx.adobe.com/security/products/xmpcore/apsb21-65.html	A-ADO-XMP_-170921/99
Heap-based Buffer Overflow	01-Sep-21	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/security/products/xmpcore/apsb21-65.html	A-ADO-XMP_-170921/100
Use After Free	01-Sep-21	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/security/products/xmpcore/apsb21-65.html	A-ADO-XMP_-170921/101
Heap-based Buffer	01-Sep-21	9.3	XMP Toolkit SDK version 2020.1 (and earlier) is	https://helpx.adobe.com/s	A-ADO-XMP_-170921/102

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/products/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/security/products/xmpcore/apsb21-65.html	A-ADO-XMP_-170921/103
Integer Overflow or Wraparound	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/security/products/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/security/prod	A-ADO-XMP_-170921/105

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Underflow')			vulnerability which 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-2021-36064**	ucts/xmpcore/apsb21-65.html	
alipay_project					
alipay					
Improper Neutralization of Special Elements used in an SQL Command ('SQL Injection')	06-Sep-21	6.5	A proid GET parameter of the WordPressæ”¯ä»˜å®?Alipay|è´¢ä»˜é€šTenpay|è´?å®?PayPalé›†æ?æ?’ä»¶ WordPress plugin through 3.7.2 is not sanitised, properly escaped or validated before inserting to a SQL statement not delimited by quotes, leading to SQL injection. **CVE ID : CVE-2021-24390**	N/A	A-ALI-ALIP-170921/106
Apache					
dubbo					
N/A	07-Sep-21	6.5	Apache Dubbo supports various rules to support configuration override or traffic routing (called routing in Dubbo). These rules are loaded into the configuration center (eg: Zookeeper, Nacos, ...) and retrieved by the customers when making a request in order to find the right endpoint. When parsing these YAML rules, Dubbo customers will use SnakeYAML library to load the rules which by default	https://lists.apache.org/thread.html/rfa351115a459e214b99ffcc52c35f33359f3370c547d9c6ba1a60037%40%3Cdev.dubbo.apache.org%3E	A-APA-DUBB-170921/107

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**		
Deserialization 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.apache.org/thread.html/r8d0adc057bb15a37199502cc366f4b1164c9c536ce28e4defdb428c0%40%3Cdev.dubbo.apache.org%3E	A-APA-DUBB-170921/108
zeppelin					
Improper Neutralization 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.apache.org/thread.html/r90590aa5ea788128ecc2e822	A-APA-ZEPP-170921/109

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Generation ('Cross-site Scripting')			This issue affects Apache Zeppelin Apache Zeppelin versions prior to 0.9.0. **CVE ID : CVE-2021-27578**	e1e64d5200b4cb92b06707b38da4cb3d%40%3Cusers.zeppelin.apache.org%3E, http://www.openwall.com/lists/oss-security/2021/09/02/3	
Apple					
safari					
Improper Authentication	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://support.apple.com/en-us/HT212529, https://support.apple.com/en-us/HT212528, https://support.apple.com/en-us/HT212534, https://support.apple.com/en-us/HT212532, https://support.apple.com/en-us/HT212533	A-APP-SAFA-170921/110
Out-of-	08-Sep-21	6.8	Multiple memory corruption	https://supp	A-APP-SAFA-

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/HT212529, https://support.apple.com/en-us/HT212528, https://support.apple.com/en-us/HT212534, https://support.apple.com/en-us/HT212532, https://support.apple.com/en-us/HT212533	170921/111
Access of Resource Using Incompatible 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://support.apple.com/en-us/HT212606, https://support.apple.com/en-us/HT212604, https://support.apple.com/en-us/HT212605, https://supp	A-APP-SAFA-170921/112

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
				ort.apple.com/en-us/HT212602, https://support.apple.com/en-us/HT212601	
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://support.apple.com/en-us/HT212606, https://support.apple.com/en-us/HT212604, https://support.apple.com/en-us/HT212605, https://support.apple.com/en-us/HT212602, https://support.apple.com/en-us/HT212601	A-APP-SAFA-170921/113
Arubanetworks					
sd-wan					
Improper Neutralization of Special	07-Sep-21	9	A remote arbitrary command execution vulnerability was discovered in Aruba SD-WAN	https://www.arubanetworks.com/asset	A-ARU-SD-W-170921/114

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Elements used in a Command ('Command Injection')			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-2021-37722**	s/alert/ARUBA-PSA-2021-016.txt	
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.arubanetworks.com/assets/alert/ARUBA-PSA-2021-016.txt	A-ARU-SD-W-170921/115
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	https://www.arubanetworks.com/assets/alert/ARUBA-PSA-2021-016.txt	A-ARU-SD-W-170921/116

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			vulnerability. **CVE ID : CVE-2021-37716**		
Improper Neutralization 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-2021-37717**	https://www.arubanetworks.com/assets/alert/ARUBA-PSA-2021-016.txt	A-ARU-SD-W-170921/117
Improper Neutralization 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.arubanetworks.com/assets/alert/ARUBA-PSA-2021-016.txt	A-ARU-SD-W-170921/118
Improper Neutralization 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.arubanetworks.com/assets/alert/ARUBA-PSA-2021-016.txt	A-ARU-SD-W-170921/119

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			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 Neutralization 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.arubanetworks.com/assets/alert/ARUBA-PSA-2021-016.txt	A-ARU-SD-W-170921/120
Improper Neutralization 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.arubanetworks.com/assets/alert/ARUBA-PSA-2021-016.txt	A-ARU-SD-W-170921/121
Atlassian					

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://bitbucket.org/atlassian/atlasboard/commits/9c03df09f09399e2601010466e8ba3a28236eb9c	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. **CVE ID : CVE-2021-39115**	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.atlassian.com/browse/JRASERVER-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

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/projectvalidate/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.atlassian.com/browse/JRASERVER-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.atlassian.com/browse/JRASERVER-72293	A-ATL-DATA-170921/127

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. **CVE ID : CVE-2021-39116**	https://jira.atlassian.com/browse/JRASERVER-72738	A-ATL-JIRA-170921/128
Improper Authentication	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/projectvalidate/key endpoint. The affected versions are before version 8.5.18, from version 8.6.0 before 8.13.10, and	https://jira.atlassian.com/browse/JRASERVER-72715	A-ATL-JIRA-170921/130

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. **CVE ID : CVE-2021-39122**	https://jira.atlassian.com/browse/JRASERVER-72293	A-ATL-JIRA-170921/131
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_windows_sender					
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

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/software/R33050099?majorVersion=2&minorVersion=5&patchVersion=3&buildVersion=65	
better_errors_project					
better_errors					
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://github.com/BetterErrors/better_errors/commit/8e8e796bfbde4aa088741823c8a3fc6df2089bb0, https://github.com/BetterErrors/better_errors/security/advisories/GHSA-w3j4-76qw-wwjm, https://github.com/BetterErrors/better_errors/pull/474	A-BET-BETT-170921/134

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			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**		
bookstackapp					
bookstack					
Server-Side Request Forgery (SSRF)	02-Sep-21	4	bookstack is vulnerable to Server-Side Request Forgery (SSRF) **CVE ID : CVE-2021-3758**	https://github.com/bookstackapp/bookstack/commit/bee5e2c7ca637d034c6985c0328cef0ce068778e, https://huntr.dev/bounties/a8d7fb24-9a69-42f3-990a-2db93b53f76b	A-BOO-BOOK-170921/135
Improper Neutralization 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-4071-8891-6183446ca980,	A-BOO-BOOK-170921/136

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Scripting')				https://github.com/bookstackapp/bookstack/commit/040997fdc4414776bcac06a3cbaac3b26b5e8a64	
Improper Neutralization 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://github.com/bookstackapp/bookstack/commit/5e6092aaf8fd4202020160382865548 60bf8ea64, https://huntr.dev/bounties/64a0229f-ff5e-4c64-b83e-9bfc0698a78e	A-BOO-BOOK-170921/137
botan_project					
botan					
Use of a Broken or Risky Cryptographic 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://github.com/randombit/botan/pull/2790	A-BOT-BOTA-170921/138

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			lead to a cross-configuration attack against OpenPGP. **CVE ID : CVE-2021-40529**		
cashtomer_project					
cashtomer					
Improper Neutralization 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					
enterprise_nfv_infrastructure_software					
Improper Authentication	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/security/center/content/CiscoSecurityAdvisory/cisco-sa-nfvis-g2DMVVh	A-CIS-ENTE-170921/140

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_programmable_network_manager					
Insufficiently 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. **CVE ID : CVE-2021-34733**	https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-prime-info-disc-nTU9FJ2	A-CIS-EVOL-170921/141
identity_services_engine					
Improper Neutralization 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/security/center/content/CiscoSecurityAdvisory/cisco-sa-ise-xss-4HnZFewr	A-CIS-IDEN-170921/142

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. **CVE ID : CVE-2021-34759**		
nexus_insights					
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/security/center/content/CiscoSecurityAdvisory/cisco-sa-insight-infodis-2By2ZpBB	A-CIS-NEXU-170921/143

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_collaboration_provisioning					
Improper Neutralization 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/security/center/content/CiscoSecurityAdvisory/cisco-sa-prime-collab-xss-fQMDE5GO	A-CIS-PRIM-170921/144
prime_infrastructure					
Insufficiently 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/security/center/content/CiscoSecurityAdvis	A-CIS-PRIM-170921/145

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. **CVE ID : CVE-2021-34733**	ory/cisco-sa-prime-info-disc-nTU9FJ2	
cliniccases					
cliniccases					
Improper Neutralization 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. **CVE ID : CVE-2021-38704**	N/A	A-CLI-CLIN-170921/146
Cross-Site Request Forgery (CSRF)	07-Sep-21	6.8	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

Weakness	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. **CVE ID : CVE-2021-38705**		
Improper Neutralization of Special Elements used in an SQL Command ('SQL Injection')	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://cliniccases.com	A-CLI-CLIN-170921/148
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	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
comment_highlighter_project					
comment_highlighter					
Improper Neutralization of Special Elements used in an	06-Sep-21	6.5	A c GET parameter of the Comment Highlighter WordPress plugin through 0.13 is not properly sanitised, escaped or validated before	N/A	A-COM-COMM-170921/150

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_order_notifications					
Improper Neutralization 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\\+\\+					
Use of a Broken or Risky Cryptographic 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

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 Synchronization ('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 Authentication	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

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_icons					
Improper Neutralization 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 Cryptographic 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.org/imap/download/release-notes/index.html,	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://github.com/cyrusimap/cyrus-imapd/commits/master, https://cyrus.topicbox.com/groups/announce/T3dde0a2352462975-M1386fc44adf967e072f8df13/cyrus-imap-3-4-2-3-2-8-and-3-0-16-released	
Deskpro					
deskpro					
Improper Neutralization 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 Neutralization 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					

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
highlight					
Improper Neutralization 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 **CVE ID : CVE-2021-24591**	N/A	A-DNA-HIGH-170921/161
easy_testimonial_manager_project					
easy_testimonial_manager					
Improper Neutralization 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/bugs/show_bug.cgi?id=568018	A-ECL-THEI-170921/163
Improper Limitation	02-Sep-21	7.5	In Eclipse Theia 0.1.1 to 0.2.0, it is possible to exploit the	https://bugs.eclipse.org/b	A-ECL-THEI-170921/164

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_bug.cgi?id=563174	
eigentech					
natural_language_processing					
Incorrect Authorization	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://eigentech.com/	A-EIG-NATU-170921/165
Incorrect Authorization	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://eigentech.com/	A-EIG-NATU-170921/166
Incorrect Authorization	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://eigentech.com/	A-EIG-NATU-170921/167

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.netcore_project					
elfinder.netcore					
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. **CVE ID : CVE-2021-23427**	N/A	A-ELF-ELFI-170921/168
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					
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

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. **CVE ID : CVE-2021-28136**	https://www.espressif.com/en/products/socs/esp32	A-ESP-ESP--170921/171
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	A-ESP-ESP--170921/172
eyoucms					
eyoucms					
Improper Neutralization 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

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 Neutralization 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					
atlant					
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	https://www.f-secure.com/en/business/programs/vulnerability-reward-program/hall-of-fame, https://www.f-	A-F-S-ATLA-170921/177

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Anti-Virus engine. **CVE ID : CVE-2021-33599**	secure.com/en/business/support-and-downloads/security-advisories/cve-2021-33599	
cloud_protection_for_salesforce					
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/en/business/programs/vulnerability-reward-program/hall-of-fame, https://www.f-secure.com/en/business/support-and-downloads/security-advisories/cve-2021-33599	A-F-S-CLOU-170921/178
elements_endpoint_protection					
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	https://www.f-secure.com/en/business/programs/vulnerability-reward-program/hall-of-fame, https://www.	A-F-S-ELEM-170921/179

Weakness	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/en/business/support-and-downloads/security-advisories/cve-2021-33599	
linux_security					
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/en/business/programs/vulnerability-reward-program/hall-of-fame, https://www.f-secure.com/en/business/support-and-downloads/security-advisories/cve-2021-33599	A-F-S-LINU-170921/180
file-upload-with-preview_project					
file-upload-with-preview					
Improper Neutralization of Input During Web Page Generation ('Cross-site	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://github.com/johndatserakis/file-upload-with-preview/pull/40/files?file-filters%5B%5D=.js&hide-	A-FIL-FILE-170921/181

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Scripting')			**CVE ID : CVE-2021-23439**	deleted-files=true%23diff-fe47b243de17419c0daa22cd785cd754baed60cf3679d3da1d6fe006f9f4a7f0R174	
Fortinet					
fortimanager					
Incorrect Authorization	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://fortiguard.com/advisory/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 **CVE ID : CVE-2021-36179**	https://fortiguard.com/advisory/FG-IR-20-206	A-FOR-FORT-170921/183
Improper Neutralization of Special Elements used in an OS	08-Sep-21	6.5	A Improper neutralization of special elements used in a command ('Command Injection') in Fortinet FortiWeb version 6.3.13 and below allows attacker to	https://fortiguard.com/advisory/FG-IR-21-047	A-FOR-FORT-170921/184

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Command ('OS Command Injection')			execute unauthorized code or commands via crafted HTTP requests **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://github.com/OpenOLAT/OpenOLAT/commit/3f219ac457afde82e3be57bc614352ab92c05684, https://github.com/OpenOLAT/OpenOLAT/security/advisories/GHSA-596v-3gwh-2m9w	A-FRE-OPEN-170921/185
gambit					
titan_framework					
Improper Neutralization of Input During Web Page Generation ('Cross-site	06-Sep-21	4.3	The iframe-font-preview.php 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

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Scripting')			issues **CVE ID : CVE-2021-24435**		
gdprinfo					
cookie_notice_\\&_consent_banner_for_gdpr_\\&_ccpa_compliance					
Improper Neutralization 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
geekwebsolution					
embed_youtube_video					
Improper Neutralization of Special Elements used in an SQL Command ('SQL Injection')	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
geminilabs					
site_reviews					
Improper Neutralization 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

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2021-24603		
ghost					
ghost					
Improper Privilege Management	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://github.com/TryGhost/Ghost/security/advisories/GHSA-j5c2-hm46-wp5c	A-GHO-GHOS-170921/190
gibbonedu					
gibbon					
Improper Neutralization 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://gibbonedu.org/	A-GIB-GIBB-170921/191

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
GNU					
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.savannah.gnu.org/cgit/inetutils.git/commit/?id=58cb043b190fd04effdaea7c9403416b436e50dd, https://lists.gnu.org/archive/html/bug-inetutils/2021-06/msg00002.html	A-GNU-INET-170921/192
Gnupg					
libgcrypt					
Use of a Broken or Risky Cryptographic 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					
chrome					

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://chromereleases.googleblog.com/2021/08/stable-channel-update-for-desktop_31.html	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://chromereleases.googleblog.com/2021/08/stable-channel-update-for-desktop_31.html	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://chromereleases.googleblog.com/2021/08/stable-channel-update-for-desktop_31.html	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://chromereleases.googleblog.com/2021/08/stable-channel-update-for-desktop_31.html	A-GOO-CHRO-170921/197
Use After	03-Sep-21	6.8	Use after free in Extensions	https://chro	A-GOO-CHRO-

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.googleblog.com/2021/08/stable-channel-update-for-desktop_31.html	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://chromereleases.googleblog.com/2021/08/stable-channel-update-for-desktop_31.html	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://chromereleases.googleblog.com/2021/08/stable-channel-update-for-desktop_31.html	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://chromereleases.googleblog.com/2021/08/stable-channel-update-for-desktop_31.html	A-GOO-CHRO-170921/201
Out-of-	03-Sep-21	6.8	Heap buffer overflow in	https://chro	A-GOO-CHRO-

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
bounds Write			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. **CVE ID : CVE-2021-30614**	mereleases.googleblog.com/2021/08/stable-channel-update-for-desktop_31.html	170921/202
Exposure of Resource to Wrong Sphere	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://chromereleases.googleblog.com/2021/08/stable-channel-update-for-desktop_31.html	A-GOO-CHRO-170921/203
Use After Free	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://chromereleases.googleblog.com/2021/08/stable-channel-update-for-desktop_31.html	A-GOO-CHRO-170921/204
N/A	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://chromereleases.googleblog.com/2021/08/stable-channel-update-for-desktop_31.html	A-GOO-CHRO-170921/205
N/A	03-Sep-21	6.8	Inappropriate implementation in DevTools in Google Chrome prior to	https://chromereleases.googleblog.co	A-GOO-CHRO-170921/206

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.html	
Authentication 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://chromereleases.googleblog.com/2021/08/stable-channel-update-for-desktop_31.html	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://chromereleases.googleblog.com/2021/08/stable-channel-update-for-desktop_31.html	A-GOO-CHRO-170921/208
Authentication 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://chromereleases.googleblog.com/2021/08/stable-channel-update-for-desktop_31.html	A-GOO-CHRO-170921/209
Use After Free	03-Sep-21	6.8	Use after free in WebApp Installs in Google Chrome prior to 93.0.4577.63 allowed an attacker who	https://chromereleases.googleblog.com/2021/08/	A-GOO-CHRO-170921/210

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.html	
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://chromereleases.googleblog.com/2021/08/stable-channel-update-for-desktop_31.html	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://chromereleases.googleblog.com/2021/08/stable-channel-update-for-desktop_31.html	A-GOO-CHRO-170921/212
Haproxy					
haproxy					
Integer Overflow or Wraparound	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.haproxy.org/?p=haproxy.git, https://github.com/haproxy/haproxy/commit/3b69886f7dcc3cfb3d166309018e6cfec9ce2c95	A-HAP-HAPR-170921/213

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
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://discuss.hashicorp.com/t/hcsec-2021-22-consul-raft-rpc-privilege-escalation/29024, https://www.hashicorp.com/blog/category/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://discuss.hashicorp.com/t/hcsec-2021-21-nomad-raft-rpc-privilege-escalation/29023, https://www.hashicorp.com/blog/category/nomad	A-HAS-NOMA-170921/215
IBM					
planning_analytics					
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/support/pages/node/6480413, https://exchange.xforce.ibmcloud.com/vulnerabilitie	A-IBM-PLAN-170921/216

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
				s/205527	
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	01-Sep-21	3.5	IBM Planning Analytics 2.0 is vulnerable to cross-site scripting. This vulnerability allows users to embed arbitrary JavaScript code in the Web UI thus altering the intended functionality potentially leading to credentials disclosure within a trusted session. IBM X-Force ID: 205528. **CVE ID : CVE-2021-29852**	https://exchange.xforce.ibmcloud.com/vulnerabilities/205528, https://www.ibm.com/support/pages/node/6480413	A-IBM-PLAN-170921/217
Unchecked Return Value	01-Sep-21	4	IBM Planning Analytics 2.0 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. **CVE ID : CVE-2021-29853**	https://exchange.xforce.ibmcloud.com/vulnerabilities/205529, https://www.ibm.com/support/pages/node/6480413	A-IBM-PLAN-170921/218
immer_project					
immer					
Access of Resource Using Incompatible Type ('Type Confusion')	01-Sep-21	7.5	This affects the package 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 ['constructor']). The ===	https://snyk.io/vuln/SNYK-JAVA-ORGWEBJARSNPM-1579266, https://snyk.io/vuln/SNYK-JS-IMMER-1540542, https://github.com/immerjs/immer/commit/fa671e	A-IMM-IMME-170921/219

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**	55ee9bd42ae08cc239102b665a23958237	
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-71e68094adfa, https://github.com/immerjs/immer/commit/fa671e55ee9bd42ae08cc239102b665a23958237	A-IMM-IMME-170921/220
ivanti					
workspace_control					
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://forums.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					

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
jforum					
Improper Neutralization 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://sourceforge.net/p/jforum2/code/934/	A-JFO-JFOR-170921/222
jiangqie					
official_website_mini_program					
Improper Neutralization 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					
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://github.com/charleskorn/kaml/issues/179, https://github.com/charleskorn/kaml/commit/e18785d043fc6324c81e968aae9764b4b060bc6a, https://github.com/charleskorn/kaml/security/advis	A-KAM-KAML-170921/224

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					
unitrends_backup_software					
Improper Privilege Management	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_meta_project					
keyword_meta					
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

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 Authorization	06-Sep-21	5.5	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. **CVE ID : CVE-2021-25735**	https://github.com/kubernetes/kubernetes/issues/100096	A-KUB-KUBE-170921/228
URL Redirection to Untrusted Site ('Open Redirect')	06-Sep-21	4.9	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 on EndpointSlice IPs. **CVE ID : CVE-2021-25737**	https://github.com/kubernetes/kubernetes/issues/102106	A-KUB-KUBE-170921/229

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
librenms					
librenms					
Improper Neutralization 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://community.librenms.org/t/vulnerability-report-cross-site-scripting-xss-in-the-api-access-page/15431, https://github.com/librenms/librenms/pull/12739	A-LIB-LIBR-170921/230
Magento					
magento					
Exposure of Sensitive Information to an Unauthorized 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/security/products/magento/apsb21-30.html	A-MAG-MAGE-170921/231
Incorrect Authorization	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/security/products/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. **CVE ID : CVE-2021-28567**		
Microfocus					
access_manager					
Exposure of Resource to Wrong Sphere	02-Sep-21	2.1	This release addresses a potential information leakage vulnerability in NetIQ Access Manager versions prior to 5.0.1 **CVE ID : CVE-2021-22525**	https://support.microfocus.com/kb/doc.php?id=7025254	A-MIC-ACCE-170921/233
network_automation					
URL Redirection to Untrusted Site ('Open Redirect')	07-Sep-21	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://portal.microfocus.com/s/article/KM000001673	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://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-	A-MIC-EDGE-170921/235

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://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2021-38642	A-MIC-EDGE-170921/236
Improper Privilege Management	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://portal.msrc.microsoft.com/en-US/security-guidance/advisory/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://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2021-26439	A-MIC-EDGE-170921/238
Improper Privilege Management	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://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2021-36930	A-MIC-EDGE-170921/239
miraheze					
globalnewfiles					
Improper Input Validation	01-Sep-21	4.3	GlobalNewFiles is a MediaWiki extension maintained by Miraheze. Prior to commit number cee254e1b158cdb0ddbea716b1d3edc31fa4fb5d, the username column of the	https://github.com/miraheze/GlobalNewFiles/security/advisories/GHSA-57p5-hqjq-h7vg,	A-MIR-GLOB-170921/240

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			GlobalNewFiles special page is vulnerable to a stored XSS. Commit number cee254e1b158cdb0ddbea716b1d3edc31fa4fb5d 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://github.com/mirahieze/GlobalNewFiles/commit/cee254e1b158cdb0ddbea716b1d3edc31fa4fb5d	
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://github.com/misskey-dev/misskey/security/advisories/GHSA-mqv7-gxh4-r5vf, https://github.com/misskey-dev/misskey/commit/e1a8b158e04ad567d92d8daf3cc0898ee18f1a2e	A-MIS-MISS-170921/241
mpath_project					
mpath					

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Access of Resource Using Incompatible Type ('Type Confusion')	01-Sep-21	7.5	This 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 ignoreProperties.indexOf(parts[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. **CVE ID : CVE-2021-23438**	https://github.com/aheckmann/mpath/commit/89402d2880d4ea3518480a8c9847c541f2d824fc	A-MPA-MPAT-170921/242
mrdoc					
mrdoc					
Deserialization of Untrusted Data	06-Sep-21	6.8	mrdoc is vulnerable to Deserialization of Untrusted Data **CVE ID : CVE-2021-32568**	https://github.com/zmister2016/mrdoc/commit/bb49e1287700b4e7681eab544c61093821ce72f6, https://huntr.dev/bounties/04fc04b3-2dc1-4cad-a090-e403cd66b5ad	A-MRD-MRDO-170921/243
myfwc					
fish_\\|_hunt_fl					

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Incorrect Authorization	08-Sep-21	4	An insecure, direct object vulnerability in hunting/fishing license retrieval function of the "Fish | Hunt FL" iOS app versions 3.8.0 and earlier allows a remote authenticated 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	08-Sep-21	5	An insufficient session 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 admin sessions. **CVE ID : CVE-2021-33982**	N/A	A-MYF-FISH-170921/245
Nextcloud					
circles					
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	07-Sep-21	3.5	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://github.com/nextcloud/security-advisories/security/advisories/GHSA-hgpq-28gj-jrj9, https://github.com/nextcloud/circles/commit/dbb97a83ccb342c839a54f088a	A-NEX-CIRC-170921/246

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**	a19b8ba6844b0e	
Authorization Bypass Through User-Controlled Key	07-Sep-21	4	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. **CVE ID : CVE-2021-37630**	https://github.com/nextcloud/security-advisories/security/advisories/GHSA-56j9-3rj4-wvgm, https://github.com/nextcloud/circles/pull/768	A-NEX-CIRC-170921/247
deck					
Authorization Bypass Through User-Controlled Key	07-Sep-21	4	Deck is an open source kanban style organization tool aimed at personal planning and project organization for teams integrated with Nextcloud. In affected versions the Deck application didn't properly check membership of users in a Circle. This allowed other users in the instance to gain access to boards that have	https://github.com/nextcloud/security-advisories/security/advisories/GHSA-4mxp-j277-82hr, https://github.com/nextcloud/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://github.com/nextcloud/security-advisories/security/advisories/GHSA-gcf3-3wmc-88jr, https://github.com/nextcloud/text/pull/1716	A-NEX-NEXT-170921/249

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 Authentication 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://github.com/nextcloud/security-advisories/security/advisories/GHSA-gv5w-8q25-785v, https://github.com/nextcloud/server/pull/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://github.com/nextcloud/security-advisories/security/advisories/GHSA-mcpf-v65v-359h	A-NEX-NEXT-170921/251

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			functionality of Nextcloud you are not affected by this bug. **CVE ID : CVE-2021-32801**		
Inclusion of Functionality from Untrusted Control Sphere	07-Sep-21	10	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**	https://github.com/nextcloud/security-advisories/security/advisories/GHSA-m682-v4g9-wrq7, https://docs.nextcloud.com/server/21/admin_manual/configuration_files/previews_configuration.html#disabling-previews	A-NEX-NEXT-170921/252
richdocuments					
Authorization Bypass Through User-	07-Sep-21	5	Nextcloud Richdocuments is an open source collaborative office suite. In affected versions the File Drop	https://github.com/nextcloud/security-advisories/se	A-NEX-RICH-170921/253

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/advisories/GHSA-pxhh-954f-8w7w, https://github.com/nextcloud/richdocuments/pull/1664	
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://github.com/nextcloud/security-advisories/security/advisories/GHSA-gvvr-h36p-8mjx	A-NEX-RICH-170921/254
objection_project					
objection					
Improperly Controlled	06-Sep-21	7.5	objection.js is vulnerable to Improperly Controlled	https://huntr.dev/bounties	A-OBJ-OBJE-170921/255

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-a1848ea031cc, https://github.com/vincit/objection.js/commit/b41aab8dcd78f426f7468dcda541a7aca18a66a6	
onyaktech_comments_pro_project					
onyaktech_comments_pro					
Improper Neutralization 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/Securing_OpenEMR	A-OPE-OPEN-170921/258
opensis_project					
opensis					
Improper Neutralization 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

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_whatprovides in src/repo.h in libsolv before 0.7.17 allows attackers to cause a Denial of Service. **CVE ID : CVE-2021-33930**	N/A	A-OPE-LIBS-170921/262
Out-of-bounds Write	02-Sep-21	5	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 Neutralization 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

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 Neutralization 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 Neutralization 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.com/release-notes/otrs-security-	A-OTR-OTRS-170921/267

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 Neutralization 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.com/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.com/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.com/release-notes/otrs-security-advisory-2021-10/	A-OTR-OTRS-170921/270

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 Management	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://owncloud.com/security-advisories/cve-2021-35946/, https://doc.owncloud.com/server/admin_manual/release_notes.html	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://owncloud.com/security-advisories/cve-2021-35947/, https://doc.owncloud.com/server/admin_manual/release_notes.html	A-OWN-OWNC-170921/272
Incorrect Authorization	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://owncloud.com/security-advisories/cve-2021-35949/, https://doc.owncloud.com/server/admi	A-OWN-OWNC-170921/273

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
				n_manual/release_notes.html	
parity					
frontier					
Improper Input Validation	03-Sep-21	5	Frontier is Substrate's Ethereum compatibility layer. Prior to commit number 0b962f218f0cdd796dadfe26c3f09e68f7861b26, 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 0b962f218f0cdd796dadfe26c3f09e68f7861b26. There are no workarounds aside from applying the patch. **CVE ID : CVE-2021-39193**	https://github.com/paritytech/frontier/pull/465/commits/8a2b890a2fb477d5fedd0e4335b00623832849ae, https://github.com/paritytech/frontier/pull/465, https://github.com/paritytech/frontier/security/advisories/GHSA-hw4v-5x4h-c3xm	A-PAR-FRON-170921/274
parseplatform					
parse-server					
Improper	02-Sep-21	5	Parse Server is an open	https://jira.m	A-PAR-PARS-

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/browse/NODE-3463, https://github.com/parse-community/parse-server/commit/308668c89474223e2448be92d6823b52c1c313ec, https://github.com/parse-community/parse-server/security/advisories/GHSA-xqp8-w826-hh6x	170921/275
pcapture_project					
pcapture					
Improper Authentication	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://github.com/jdhwpgmbca/pcapture/security/advisories/GHSA-3r67-fxpr-p2qx, https://github.com/jdhwpgmbca/pcapture/issues/7, https://github.com/jdhwpgmbca/pcapture/commit/0f74f431e0970a2e5784db	A-PCA-PCAP-170921/276

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. **CVE ID : CVE-2021-39196**	d955cfa4760e3b1ef7	
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 Neutralization 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://github.com/pimcore/pimcore/security/advisories/GHSA-w6j8-jc36-x5q9, https://github.com/pimcore/pimcore/pull/10170	A-PIM-PIMC-170921/278
Improper Neutralization 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://github.com/pimcore/pimcore/pull/10178.pat	A-PIM-PIMC-170921/279

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://github.com/pimcore/pimcore/pull/10178, https://github.com/pimcore/pimcore/security/advisories/GHSA-2v88-qq7x-xq5f, https://huntr.dev/bounties/e4cb9cd8-89cf-427c-8d2e-37ca40099bf2/	
proto_project					
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://puppet.com/security/cve/CVE-2021-27022/	A-PUP-PUPP-170921/281

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. **CVE ID : CVE-2021-40524**	N/A	A-PUR-PURE-170921/282
Python					
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://pillow.readthedocs.io/en/stable/releasenotes/8.3.2.html, https://github.com/python-pillow/Pillow/commit/9e08eb8f78fdfd2f476e1b20b7cf38683754866b, https://snyk.io/vuln/SNYK-PYTHON-PILLOW-1319443	A-PYT-PILL-170921/283

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
redux					
gutenberg_template_library_\\&_redux_framework					
Incorrect Authorization	02-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

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					
remark-html					
Improper Neutralization 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://github.com/remarkjs/remark-html/releases/tag/14.0.1, https://github.com/remarkjs/remark-html/security/advisories/GHSA-9q5w-79cv-947m, https://github.com/remarkjs/remark-html/commit/b75c9dde582ad87ba498e369c033dc8a350478c1	A-REM-REMA-170921/286
Samsung					
drive_manager					

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Incorrect Authorization	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-electric					
gp-pro_ex					
Uncontrolled 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://download.schneider-electric.com/files?p_Doc_Ref=SEVD-2021-222-03	A-SCH-GP-P-170921/288
simple_water_refilling_station_management_system_project					
simple_water_refilling_station_management_system					
Improper Neutralization 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

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Type			Logo option on the system_info page in classes/SystemSettings.php with an update_settings action. **CVE ID : CVE-2021-38841**		
Sketch					
sketch					
N/A	06-Sep-21	7.5	Sketch before 75 mishandles external library feeds. **CVE ID : CVE-2021-40531**	https://www.sketch.com/updates/#version-75	A-SKE-SKET-170921/291
Smartertools					
smartermail					
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	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/smartermail/release-notes/current	A-SMA-SMAR-170921/292
Solarwinds					
orion_platform					
Deserialization of Untrusted Data	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://documentation.solarwinds.com/en/success_center/orionplatform/content/core-secure-configuration.htm, https://www.	A-SOL-ORIO-170921/293

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
				solarwinds.com/trust-center/security-advisories/cve-2021-35215	
Deserialization 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://documentation.solarwinds.com/en/success_center/patchman/content/release_notes/patchman_2020-2-6_release_notes.htm, https://www.solarwinds.com/trust-center/security-advisories/cve-2021-35218	A-SOL-ORIO-170921/294
Improper Neutralization 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://support.solarwinds.com/SuccessCenter/s/article/Orion-Platform-2020-2-6-Hotfix-1?language=en_US, https://documentation.solarwinds.com/en/success_c	A-SOL-ORIO-170921/295

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
				enter/orionplatform/content/core-secure-configuration.htm	
patch_manager					
Deserialization of Untrusted Data	01-Sep-21	9	Insecure Deserialization of untrusted data remote code execution vulnerability was discovered in Patch Manager Orion Platform Integration module. An Authenticated Attacker with network access via HTTP can compromise this vulnerability can result in Remote Code Execution. **CVE ID : CVE-2021-35216**	https://documentation.solarwinds.com/en/success_center/patchman/content/release_notes/patchman_2020-2-6_release_notes.htm, https://www.solarwinds.com/trust-center/security-advisories/cve-2021-35216	A-SOL-PATC-170921/296
Sonatype					
nexus_repository_manager_3					
Improper Neutralization of Special Elements in Output Used by a Downstream Component ('Injection')	07-Sep-21	6.4	Sonatype Nexus Repository 3.x through 3.33.1-01 is vulnerable to an HTTP header injection. By sending a crafted HTTP request, a remote attacker may disclose sensitive information or request external resources from a vulnerable instance. **CVE ID : CVE-2021-40143**	https://support.sonatype.com/hc/en-us/articles/440594176257 9	A-SON-NEXU-170921/297

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
sqlite-web_project					
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					
club-management-software					
Improper Neutralization 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://github.com/morethanwords/tweb/commit/f224e459c36eb96b2cf9dba559a48b1f08d23330	A-TEL-WEB_-170921/300

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
terarecon					
aquariusnet					
Improper Privilege Management	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					
covid-19_contact_tracing					
Improper Authentication	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/studieren-weiterbilden/neuigkeiten-und-veranstaltungen/corona/	A-TH--COVI-170921/302
Trendmicro					
maximum_security_2019					
Improper Privilege Management	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://helpcenter.trendmicro.com/en-us/article/tmka-10568	A-TRE-MAXI-170921/303

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
maximum_security_2020					
Improper Privilege Management	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://helpcenter.trendmicro.com/en-us/article/tmka-10568	A-TRE-MAXI-170921/304
maximum_security_2021					
Improper Privilege Management	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://helpcenter.trendmicro.com/en-us/article/tmka-10568	A-TRE-MAXI-170921/305
security_for_best_buy					
Improper Privilege Management	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://helpcenter.trendmicro.com/en-us/article/tmka-10568	A-TRE-SECU-170921/306
trumani					
stop_spammers					
Improper Neutralization 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

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					
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://github.com/http4s/http4s/security/advisories/GHSA-52cf-226f-rhr6	A-TYP-HTTP-170921/308
ulfius_project					
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://github.com/babelouest/ulfius/commit/c83f564c184a2714	A-ULF-ULFI-170921/309

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			certain malformed HTTP requests. **CVE ID : CVE-2021-40540**	5e07c274b305cabe943bbfaa, https://github.com/babelouest/ulfius/compare/v2.7.3...v2.7.4	
underconstruction_project					
underconstruction					
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	01-Sep-21	4.3	The 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. **CVE ID : CVE-2021-39320**	N/A	A-UND-UNDE-170921/310
versa-networks					
versa_director					
Improper Neutralization 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.com	A-VER-VERS-170921/311
VIM					
vim					
Out-of-bounds	06-Sep-21	4.6	vim is vulnerable to Heap-based Buffer Overflow	https://github.com/vim/vi	A-VIM-VIM-170921/312

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Write			**CVE ID : CVE-2021-3770**	m/commit/b7081e135a16091c93f6f5f7525a5c58fb7ca9f9, https://huntr.dev/bounties/016ad2f2-07c1-4d14-a8ce-6eed10729365	
web-settler					
form_builder					
Improper Neutralization 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					
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://weechat.org/doc/security/, https://github.com/weechat/weechat/commit/8b1331f98de1714bae15a9ca2e2b393ba49d	A-WEE-WEEC-170921/314

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
				735b	
wp-webhooks					
email_encoder					
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	06-Sep-21	4.3	The Email Encoder â€“ 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-WP--EMAI-170921/315
wpfront					
wpfront_notification_bar					
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	06-Sep-21	3.5	The WPFront Notification Bar WordPress plugin before 2.1.0.08087 does not properly sanitise and escape its settings, which could allow high privilege users to perform Cross-Site Scripting attacks even when the unfiltered_html capability is disallowed. **CVE ID : CVE-2021-24601**	N/A	A-WPF-WPFR-170921/316
zmartzone					
mod_auth_openidc					
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://github.com/zmartzone/mod_auth_openidc/commit/03e6bfb446f4e3f27c003d30d6a433e5dd8e2b3d,	A-ZMA-MOD_-170921/317

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://github.com/zmartzone/mod_auth_openidc/security/advisories/GHSA-2pgf-8h6h-gqg2	
Zohocorp					
manageengine_adselfservice_plus					
Improper Authentication	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.manageengine.com/products/self-service-password/kb/how-to-fix-authentication-bypass-vulnerability-in-REST-API.html, https://www.manageengine.com	A-ZOH-MANA-170921/318
manageengine_servicedesk_plus					
Improper Authentication	01-Sep-21	7.5	Zoho ManageEngine ServiceDesk Plus before 11302 is vulnerable to authentication bypass that	https://www.manageengine.com, https://www.	A-ZOH-MANA-170921/319

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			allows a few REST-API URLs without authentication. **CVE ID : CVE-2021-37415**	manageengine.com/products/service-desk/on-premises/readme.html#11302	
Hardware					
actions-semi					
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/index.php?id=3581&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/index.php?id=3581&siteId=4	H-ACT-ATS2-170921/321

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			matches the original connected host. **CVE ID : CVE-2021-31786**		
ats2819					
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/index.php?id=3581&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/index.php?id=3581&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-

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/index.php?id=3581&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/index.php?id=3581&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/index.php?id=3581&siteId=4	H-ACT-ATS2-170921/326

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/index.php?id=3581&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/index.php?id=3581&siteId=4	H-ACT-ATS2-170921/328

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 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/index.php?id=3581&siteId=4	H-ACT-ATS2-170921/329
Amazon					
kindle					
Integer Overflow or Wraparound	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 Management	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

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
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. **CVE ID : CVE-2021-37731**	https://www.arubanetworks.com/assets/alert/ARUBA-PSA-2021-016.txt	H-ARU-7005-170921/332
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.arubanetworks.com/assets/alert/ARUBA-PSA-2021-016.txt	H-ARU-7008-170921/333
7010					
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.arubanetworks.com/assets/alert/ARUBA-PSA-2021-	H-ARU-7010-170921/334

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					
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.arubanetworks.com/assets/alert/ARUBA-PSA-2021-016.txt	H-ARU-7024-170921/335
7030					
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.arubanetworks.com/assets/alert/ARUBA-PSA-2021-016.txt	H-ARU-7030-170921/336

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
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.arubanetworks.com/assets/alert/ARUBA-PSA-2021-016.txt	H-ARU-7205-170921/337
7210					
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.arubanetworks.com/assets/alert/ARUBA-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.arubanetworks.com/assets/alert/ARUBA-PSA-2021-016.txt	H-ARU-7220-170921/339

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					
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.arubanetworks.com/assets/alert/ARUBA-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.arubanetworks.com/assets/alert/ARUBA-PSA-2021-016.txt	H-ARU-7280-170921/341

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
9004					
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.arubanetworks.com/assets/alert/ARUBA-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.arubanetworks.com/assets/alert/ARUBA-PSA-2021-016.txt	H-ARU-9004-170921/343
9012					
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.arubanetworks.com/assets/alert/ARUBA-PSA-2021-016.txt	H-ARU-9012-170921/344

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**		
bluetrum					
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.com/product/ab5301a.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.com/product/ab5376t.html, http://www.bluetrum.com/product/bt8896a.html	H-BLU-AB53-170921/346

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**		
bt8896a					
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.com/product/ab5376t.html, http://www.bluetrum.com/product/bt8896a.html	H-BLU-BT88-170921/347
christiedigital					
dwu850-gs					
Improper Authentication	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					
Missing Authorization	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

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			deletes all data from the device. **CVE ID : CVE-2021-40378**		
Improper Privilege Management	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 Authentication	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 Management	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 Management	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					
Missing Authorization	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

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 Management	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 Authentication	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 Management	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 Management	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					
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

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 Management	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 Authentication	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 Management	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 Management	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-

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. **CVE ID : CVE-2021-40378**		170921/364
Improper Privilege Management	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
Improper Authentication	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-TN54-170921/366
Improper Privilege Management	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-TN54-170921/367
Improper Privilege Management	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					

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
cyw20735b1					
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 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 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**	https://www.cypress.com/documentation/datasheets/cyw20735b1-single-chip-bluetooth-transceiver-wireless-input-devices	H-CYP-CYW2-170921/369
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/documentation/datasheets/cyw20735b1-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/documentation/datasheets/cyw20735b1-single-chip-bluetooth-transceiver-	H-CYP-CYW2-170921/371

Weakness	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	
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 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. **CVE ID : CVE-2021-34148**	https://www.cypress.com/documentation/datasheets/cyw20735b1-single-chip-bluetooth-transceiver-wireless-input-devices	H-CYP-CYW2-170921/372
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/documentation/datasheets/cyw20735b1-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					
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/over-ear-headphones/J	H-JBL-TUNE-170921/376

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			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**	BL+TUNE500BT.html	
kpn					
experia_wifi					
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/producten/experia-wifi/2	H-KPN-EXPE-170921/377
mi					
mi_true_wireless_earbuds_basic_2					
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	http://www.bluetrum.com/product/ab5376t.html, http://www.bluetrum.com/product/bt8896a.html	H-MI-MI_T-170921/378

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			with LMP_AU_rand data. **CVE ID : CVE-2021-31610**		
Moxa					
oncell_g3470a-lte-eu					
Improper Neutralization 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-ONCE-170921/379
Improper Neutralization 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_g3470a-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

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 Neutralization 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-ct-t					
Improper Neutralization 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

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 Neutralization 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					
Improper Neutralization 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 Neutralization of Special	07-Sep-21	9	Certain MOXA devices allow Authenticated Command Injection via	https://www.moxa.com	H-MOX-TAP--170921/386

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Elements used in an OS Command ('OS Command Injection')			/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**		
tap-323-us-ct-t					
Improper Neutralization 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--170921/387
Improper Neutralization 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-	https://www.moxa.com	H-MOX-TAP--170921/388

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					
Improper Neutralization 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 Neutralization 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					

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Improper Neutralization 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 Neutralization 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 Neutralization 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

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Scripting')			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 Neutralization 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--170921/394
wdr-3124a-eu					
Improper Neutralization 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--170921/395
Improper	07-Sep-21	9	Certain MOXA devices allow	https://www.	H-MOX-WDR-

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Neutralization 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. **CVE ID : CVE-2021-39279**	moxa.com	-170921/396
wdr-3124a-eu-t					
Improper Neutralization 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 Neutralization 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

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-us					
Improper Neutralization 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 Neutralization 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-us-t					
Improper Neutralization 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 Neutralization 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/security/products/medium/apsb21-	H-OCU-RIFT-170921/403

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					
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/security/products/medium/apsb21-34.html	H-OCU-RIFT-170921/404
touch					
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/security/products/medium/apsb21-34.html	H-OCU-TOUC-170921/405

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					
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.com/company/product-security/bulletins/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.com/company/product-security/bulletins/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.com/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 **CVE ID : CVE-2021-1916**	etins/august-2021-bulletin	
Integer Underflow (Wrap or Wraparound)	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.com/company/product-security/bulletins/august-2021-bulletin	H-QUA-APQ8-170921/409
Integer Underflow (Wrap or Wraparound)	08-Sep-21	10	Integer underflow can occur due to improper 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.com/company/product-security/bulletins/august-2021-bulletin	H-QUA-APQ8-170921/410
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.com/company/product-security/bulletins/august-	H-QUA-APQ8-170921/411

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1928**	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 Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1972**	https://www.qualcomm.com/company/product-security/bulletins/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 **CVE ID : CVE-2021-1904**	https://www.qualcomm.com/company/product-security/bulletins/august-2021-bulletin	H-QUA-APQ8-170921/413
Loop with	08-Sep-21	5	Loop with unreachable exit	https://www.	H-QUA-APQ8-

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.com/company/product-security/bulletins/august-2021-bulletin	170921/414
Out-of-bounds Write	08-Sep-21	10	Possible buffer underflow due to lack of check for negative indices values when 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.com/company/product-security/bulletins/august-2021-bulletin	H-QUA-APQ8-170921/415
Integer Underflow (Wrap or Wraparound)	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.com/company/product-security/bulletins/august-2021-bulletin	H-QUA-APQ8-170921/416
Integer	08-Sep-21	10	Integer underflow can occur	https://www.	H-QUA-APQ8-

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Underflow (Wrap or Wraparound)			due to improper 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.com/company/product-security/bulletins/august-2021-bulletin	170921/417
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	08-Sep-21	10	Possible buffer overflow due to 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 Networking **CVE ID : CVE-2021-1972**	https://www.qualcomm.com/company/product-security/bulletins/august-2021-bulletin	H-QUA-APQ8-170921/418
apq8017					
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.com/company/product-security/bulletins/august-2021-bulletin	H-QUA-APQ8-170921/419

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.com/company/product-security/bulletins/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.com/company/product-security/bulletins/august-2021-bulletin	H-QUA-APQ8-170921/421
Integer Underflow (Wrap or Wraparound)	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.com/company/product-security/bulletins/august-2021-bulletin	H-QUA-APQ8-170921/422

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Wearables **CVE ID : CVE-2021-1919**		
Integer Underflow (Wrap or Wraparound)	08-Sep-21	10	Integer underflow can occur due to improper 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.com/company/product-security/bulletins/august-2021-bulletin	H-QUA-APQ8-170921/423
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	08-Sep-21	10	Possible buffer overflow due to 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 Networking **CVE ID : CVE-2021-1972**	https://www.qualcomm.com/company/product-security/bulletins/august-2021-bulletin	H-QUA-APQ8-170921/424
apq8037					
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.com/company/product-security/bulletins/august-2021-bulletin	H-QUA-APQ8-170921/425

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.com/company/product-security/bulletins/august-2021-bulletin	H-QUA-APQ8-170921/426
Integer Underflow (Wrap or Wraparound)	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.com/company/product-security/bulletins/august-2021-bulletin	H-QUA-APQ8-170921/427
Integer Underflow (Wrap or Wraparound)	08-Sep-21	10	Integer 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.com/company/product-security/bulletins/august-2021-bulletin	H-QUA-APQ8-170921/428

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 Voice & Music, Snapdragon Wearables **CVE ID : CVE-2021-1904**	https://www.qualcomm.com/company/product-security/bulletins/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.com/company/product-security/bulletins/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.com/company/product-security/bulletins/august-	H-QUA-APQ8-170921/431

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-2021-1916**	2021-bulletin	
Integer Underflow (Wrap or Wraparound)	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.com/company/product-security/bulletins/august-2021-bulletin	H-QUA-APQ8-170921/432
Integer Underflow (Wrap or Wraparound)	08-Sep-21	10	Integer underflow can occur due to improper 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.com/company/product-security/bulletins/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.com/company/product-security/bulletins/august-2021-bulletin	H-QUA-APQ8-170921/434

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 Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1972**	https://www.qualcomm.com/company/product-security/bulletins/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 Voice & Music, Snapdragon Wearables **CVE ID : CVE-2021-1904**	https://www.qualcomm.com/company/product-security/bulletins/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 Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1972**	m/company/product-security/bulletins/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.com/company/product-security/bulletins/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.com/company/product-security/bulletins/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					
Out-of-bounds Write	08-Sep-21	10	Possible buffer underflow due to lack of check for negative indices values when 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.com/company/product-security/bulletins/august-2021-bulletin	H-QUA-APQ8-170921/440
Integer Underflow (Wrap or Wraparound)	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.com/company/product-security/bulletins/august-2021-bulletin	H-QUA-APQ8-170921/441
Integer Underflow (Wrap or Wraparound)	08-Sep-21	10	Integer 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.com/company/product-security/bulletins/august-2021-bulletin	H-QUA-APQ8-170921/442

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 Voice & Music, Snapdragon Wearables **CVE ID : CVE-2021-1904**	https://www.qualcomm.com/company/product-security/bulletins/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.com/company/product-security/bulletins/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.com/company/product-security/bulletins/august-	H-QUA-APQ8-170921/445

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-2021-1916**	2021-bulletin	
Integer Underflow (Wrap or Wraparound)	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.com/company/product-security/bulletins/august-2021-bulletin	H-QUA-APQ8-170921/446
Integer Underflow (Wrap or Wraparound)	08-Sep-21	10	Integer underflow can occur due to improper 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.com/company/product-security/bulletins/august-2021-bulletin	H-QUA-APQ8-170921/447
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.com/company/product-security/bulletins/august-2021-bulletin	H-QUA-APQ8-170921/448

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 Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1972**	https://www.qualcomm.com/company/product-security/bulletins/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 Voice & Music, Snapdragon Wearables **CVE ID : CVE-2021-1904**	https://www.qualcomm.com/company/product-security/bulletins/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.com/company/product-	H-QUA-AQT1-170921/451

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/bulletins/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.com/company/product-security/bulletins/august-2021-bulletin	H-QUA-AQT1-170921/452
Integer Underflow (Wrap or Wraparound)	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.com/company/product-security/bulletins/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.com/company/product-	H-QUA-AQT1-170921/454

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/bulletins/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.com/company/product-security/bulletins/august-2021-bulletin	H-QUA-AQT1-170921/455
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.com/company/product-security/bulletins/august-2021-bulletin	H-QUA-AQT1-170921/456
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.com/company/product-security/bulletins/august-2021-bulletin	H-QUA-AQT1-170921/457

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 Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1972**	https://www.qualcomm.com/company/product-security/bulletins/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.com/company/product-security/bulletins/august-2021-bulletin	H-QUA-AR60-170921/459
Integer Underflow (Wrap or Wraparound)	08-Sep-21	10	Integer underflow can occur due to improper 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.com/company/product-security/bulletins/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 Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1972**	https://www.qualcomm.com/company/product-security/bulletins/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 Mobile, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1972**	https://www.qualcomm.com/company/product-security/bulletins/august-2021-bulletin	H-QUA-AR74-170921/462
ar8031					
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.com/company/product-	H-QUA-AR80-170921/463

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/bulletins/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 Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1972**	https://www.qualcomm.com/company/product-security/bulletins/august-2021-bulletin	H-QUA-AR80-170921/464
ar8035					
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.com/company/product-security/bulletins/august-2021-bulletin	H-QUA-AR80-170921/465

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 Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1972**	https://www.qualcomm.com/company/product-security/bulletins/august-2021-bulletin	H-QUA-AR80-170921/466
ar9380					
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.com/company/product-security/bulletins/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.com/company/product-security/bulletins/august-2021-bulletin	H-QUA-AR93-170921/468

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**		
csr6030					
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.com/company/product-security/bulletins/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.com/company/product-security/bulletins/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/bulletins/august-2021-bulletin	
Integer Underflow (Wrap or Wraparound)	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.com/company/product-security/bulletins/august-2021-bulletin	H-QUA-CSR6-170921/472
Integer Underflow (Wrap or Wraparound)	08-Sep-21	10	Integer underflow can occur due to improper 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.com/company/product-security/bulletins/august-2021-bulletin	H-QUA-CSR6-170921/473
Buffer Copy without Checking	08-Sep-21	10	Possible buffer overflow due to improper validation of device types during P2P	https://www.qualcomm.com/company/	H-QUA-CSR6-170921/474

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/bulletins/august-2021-bulletin	
csr8811					
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.com/company/product-security/bulletins/august-2021-bulletin	H-QUA-CSR8-170921/475
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	08-Sep-21	10	Possible buffer overflow due to 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	https://www.qualcomm.com/company/product-security/bulletins/august-2021-bulletin	H-QUA-CSR8-170921/476

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 Voice & Music, Snapdragon Wearables **CVE ID : CVE-2021-1904**	https://www.qualcomm.com/company/product-security/bulletins/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 Mobile, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1972**	https://www.qualcomm.com/company/product-security/bulletins/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.com/company/product-security/bull	H-QUA-CSRA-170921/479

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 Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1972**	https://www.qualcomm.com/company/product-security/bulletins/august-2021-bulletin	H-QUA-CSRA-170921/480
csrb31024					
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.com/company/product-security/bulletins/august-2021-bulletin	H-QUA-CSRB-170921/481

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 IoT, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2021-1914**	https://www.qualcomm.com/company/product-security/bulletins/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.com/company/product-security/bulletins/august-2021-bulletin	H-QUA-CSRB-170921/483
Integer Underflow (Wrap or Wraparound)	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.com/company/product-security/bulletins/august-2021-bulletin	H-QUA-CSRB-170921/484

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2021-1919		
Integer Underflow (Wrap or Wraparound)	08-Sep-21	10	Integer underflow can occur due to improper 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.com/company/product-security/bulletins/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.com/company/product-security/bulletins/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 Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1972**	https://www.qualcomm.com/company/product-security/bulletins/august-2021-bulletin	H-QUA-CSRB-170921/487

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
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 Voice & Music, Snapdragon Wearables **CVE ID : CVE-2021-1904**	https://www.qualcomm.com/company/product-security/bulletins/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 Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1972**	https://www.qualcomm.com/company/product-security/bulletins/august-2021-bulletin	H-QUA-FSM1-170921/489
fsm10056					
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.com/company/product-security/bulletins/august-2021-bulletin	H-QUA-FSM1-170921/490

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 Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1972**	https://www.qualcomm.com/company/product-security/bulletins/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.com/company/product-security/bulletins/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 Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1972**	m/company/product-security/bulletins/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.com/company/product-security/bulletins/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 Voice & Music, Snapdragon Wearables, Snapdragon Wired	https://www.qualcomm.com/company/product-security/bulletins/august-2021-bulletin	H-QUA-IPQ4-170921/495

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Infrastructure and Networking **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.com/company/product-security/bulletins/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 Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1972**	https://www.qualcomm.com/company/product-security/bulletins/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.com/company/product-security/bull	H-QUA-IPQ4-170921/498

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 Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1972**	https://www.qualcomm.com/company/product-security/bulletins/august-2021-bulletin	H-QUA-IPQ4-170921/499
ipq5010					
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.com/company/product-security/bulletins/august-2021-bulletin	H-QUA-IPQ5-170921/500
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 Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1972**	qualcomm.com/company/product-security/bulletins/august-2021-bulletin	170921/501
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.com/company/product-security/bulletins/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.com/company/product-security/bulletins/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 Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1972**	https://www.qualcomm.com/company/product-security/bulletins/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.com/company/product-security/bulletins/august-2021-bulletin	H-QUA-IPQ6-170921/505
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.com/company/product-	H-QUA-IPQ6-170921/506

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/bulletins/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.com/company/product-security/bulletins/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 Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and	https://www.qualcomm.com/company/product-security/bulletins/august-2021-bulletin	H-QUA-IPQ6-170921/508

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Networking **CVE ID : CVE-2021-1972**		
ipq6010					
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.com/company/product-security/bulletins/august-2021-bulletin	H-QUA-IPQ6-170921/509
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	08-Sep-21	10	Possible buffer overflow due to 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 Networking **CVE ID : CVE-2021-1972**	https://www.qualcomm.com/company/product-security/bulletins/august-2021-bulletin	H-QUA-IPQ6-170921/510
ipq6018					
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.com/company/product-security/bulletins/august-	H-QUA-IPQ6-170921/511

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1928**	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 Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1972**	https://www.qualcomm.com/company/product-security/bulletins/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.com/company/product-security/bulletins/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 Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1972**	m/company/product-security/bulletins/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 **CVE ID : CVE-2021-1928**	https://www.qualcomm.com/company/product-security/bulletins/august-2021-bulletin	H-QUA-IPQ8-170921/515
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	08-Sep-21	10	Possible buffer overflow due to 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	https://www.qualcomm.com/company/product-security/bulletins/august-2021-bulletin	H-QUA-IPQ8-170921/516

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Infrastructure and Networking **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.com/company/product-security/bulletins/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 Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1972**	https://www.qualcomm.com/company/product-security/bulletins/august-2021-bulletin	H-QUA-IPQ8-170921/518
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.com/company/product-security/bull	H-QUA-IPQ8-170921/519

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 Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1972**	https://www.qualcomm.com/company/product-security/bulletins/august-2021-bulletin	H-QUA-IPQ8-170921/520
ipq8069					
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.com/company/product-security/bulletins/august-2021-bulletin	H-QUA-IPQ8-170921/521
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')			to 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 Networking **CVE ID : CVE-2021-1972**	qualcomm.com/company/product-security/bulletins/august-2021-bulletin	170921/522
ipq8070					
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.com/company/product-security/bulletins/august-2021-bulletin	H-QUA-IPQ8-170921/523
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	08-Sep-21	10	Possible buffer overflow due to 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.com/company/product-security/bulletins/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 **CVE ID : CVE-2021-1928**	https://www.qualcomm.com/company/product-security/bulletins/august-2021-bulletin	H-QUA-IPQ8-170921/525
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	08-Sep-21	10	Possible buffer overflow due to 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 Networking **CVE ID : CVE-2021-1972**	https://www.qualcomm.com/company/product-security/bulletins/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.com/company/product-	H-QUA-IPQ8-170921/527

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/bulletins/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 Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1972**	https://www.qualcomm.com/company/product-security/bulletins/august-2021-bulletin	H-QUA-IPQ8-170921/528
ipq8071a					
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.com/company/product-security/bulletins/august-2021-bulletin	H-QUA-IPQ8-170921/529

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 Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1972**	https://www.qualcomm.com/company/product-security/bulletins/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.com/company/product-security/bulletins/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.com/company/product-security/bulletins/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					
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.com/company/product-security/bulletins/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 Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1972**	https://www.qualcomm.com/company/product-security/bulletins/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.com/company/	H-QUA-IPQ8-170921/535

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/bulletins/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 Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1972**	https://www.qualcomm.com/company/product-security/bulletins/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.com/company/product-security/bulletins/august-2021-bulletin	H-QUA-IPQ8-170921/537

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 Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1972**	https://www.qualcomm.com/company/product-security/bulletins/august-2021-bulletin	H-QUA-IPQ8-170921/538
ipq8076					
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.com/company/product-security/bulletins/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.com/company/product-security/bulletins/august-2021-bulletin	H-QUA-IPQ8-170921/540

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.com/company/product-security/bulletins/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 Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1972**	https://www.qualcomm.com/company/product-security/bulletins/august-2021-bulletin	H-QUA-IPQ8-170921/542
ipq8078					

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.com/company/product-security/bulletins/august-2021-bulletin	H-QUA-IPQ8-170921/543
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	08-Sep-21	10	Possible buffer overflow due to 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 Networking **CVE ID : CVE-2021-1972**	https://www.qualcomm.com/company/product-security/bulletins/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.com/company/product-security/bulletins/august-2021-bulletin	H-QUA-IPQ8-170921/545

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 Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1972**	https://www.qualcomm.com/company/product-security/bulletins/august-2021-bulletin	H-QUA-IPQ8-170921/546
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.com/company/product-security/bulletins/august-2021-bulletin	H-QUA-IPQ8-170921/547
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.com/company/product-security/bulletins/august-	H-QUA-IPQ8-170921/548

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					
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.com/company/product-security/bulletins/august-2021-bulletin	H-QUA-IPQ8-170921/549
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	08-Sep-21	10	Possible buffer overflow due to 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 Networking **CVE ID : CVE-2021-1972**	https://www.qualcomm.com/company/product-security/bulletins/august-2021-bulletin	H-QUA-IPQ8-170921/550

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
mdm8207					
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.com/company/product-security/bulletins/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.com/company/product-security/bulletins/august-2021-bulletin	H-QUA-MDM8-170921/552
Integer Underflow (Wrap or Wraparound)	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.com/company/product-security/bulletins/august-2021-bulletin	H-QUA-MDM8-170921/553

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2021-1919		
Integer Underflow (Wrap or Wraparound)	08-Sep-21	10	Integer underflow can occur due to improper 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.com/company/product-security/bulletins/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.com/company/product-security/bulletins/august-2021-bulletin	H-QUA-MDM8-170921/555
Integer Underflow (Wrap or Wraparound)	08-Sep-21	10	Integer underflow can occur due to improper 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.com/company/product-security/bulletins/august-2021-bulletin	H-QUA-MDM8-170921/556

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 Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1972**	https://www.qualcomm.com/company/product-security/bulletins/august-2021-bulletin	H-QUA-MDM8-170921/557
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.com/company/product-security/bulletins/august-2021-bulletin	H-QUA-MDM8-170921/558
Integer Underflow (Wrap or Wraparound)	08-Sep-21	10	Integer 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.com/company/product-security/bulletins/august-2021-bulletin	H-QUA-MDM8-170921/559

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 Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1972**	https://www.qualcomm.com/company/product-security/bulletins/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.com/company/product-security/bulletins/august-2021-bulletin	H-QUA-MDM8-170921/561
Integer Underflow (Wrap or Wraparound)	08-Sep-21	10	Integer underflow can occur due to improper handling of incoming RTCP packets in Snapdragon Auto, Snapdragon Compute,	https://www.qualcomm.com/company/product-security/bull	H-QUA-MDM8-170921/562

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-2021-1920**	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 Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1972**	https://www.qualcomm.com/company/product-security/bulletins/august-2021-bulletin	H-QUA-MDM8-170921/563
mdm9150					
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.com/company/product-security/bulletins/august-2021-bulletin	H-QUA-MDM9-170921/564
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 **CVE ID : CVE-2021-1914**	qualcomm.com/company/product-security/bulletins/august-2021-bulletin	MDM9-170921/565
Out-of-bounds Write	08-Sep-21	10	Possible buffer underflow due to lack of check for negative indices values when 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.com/company/product-security/bulletins/august-2021-bulletin	H-QUA-MDM9-170921/566
Integer Underflow (Wrap or Wraparound)	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.com/company/product-security/bulletins/august-2021-bulletin	H-QUA-MDM9-170921/567
Integer	08-Sep-21	10	Integer underflow can occur	https://www.	H-QUA-

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Underflow (Wrap or Wraparound)			due to improper 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.com/company/product-security/bulletins/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 Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1972**	https://www.qualcomm.com/company/product-security/bulletins/august-2021-bulletin	H-QUA-MDM9-170921/569
mdm9205					
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.com/company/product-security/bulletins/august-2021-bulletin	H-QUA-MDM9-170921/570

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 **CVE ID : CVE-2021-1916**	https://www.qualcomm.com/company/product-security/bulletins/august-2021-bulletin	H-QUA-MDM9-170921/571
Integer Underflow (Wrap or Wraparound)	08-Sep-21	10	Integer underflow can occur due to improper 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.com/company/product-security/bulletins/august-2021-bulletin	H-QUA-MDM9-170921/572
mdm9206					
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.com/company/product-security/bulletins/august-2021-bulletin	H-QUA-MDM9-170921/573

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.com/company/product-security/bulletins/august-2021-bulletin	H-QUA-MDM9-170921/574
Out-of-bounds Write	08-Sep-21	10	Possible buffer underflow due to lack of check for negative indices values when 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.com/company/product-security/bulletins/august-2021-bulletin	H-QUA-MDM9-170921/575
Integer Underflow (Wrap or Wraparound)	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.com/company/product-security/bulletins/august-2021-bulletin	H-QUA-MDM9-170921/576

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 Wraparound)	08-Sep-21	10	Integer underflow can occur due to improper 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.com/company/product-security/bulletins/august-2021-bulletin	H-QUA-MDM9-170921/577
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.com/company/product-security/bulletins/august-2021-bulletin	H-QUA-MDM9-170921/578
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	08-Sep-21	10	Possible buffer overflow due 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.com/company/product-security/bulletins/august-2021-bulletin	H-QUA-MDM9-170921/579

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.com/company/product-security/bulletins/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.com/company/product-security/bulletins/august-2021-bulletin	H-QUA-MDM9-170921/581
Integer Underflow (Wrap or Wraparound)	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.com/company/product-security/bull	H-QUA-MDM9-170921/582

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-2021-1919**	etins/august-2021-bulletin	
Integer Underflow (Wrap or Wraparound)	08-Sep-21	10	Integer underflow can occur due to improper 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.com/company/product-security/bulletins/august-2021-bulletin	H-QUA-MDM9-170921/583
mdm9215					
Out-of-bounds Write	08-Sep-21	10	Possible buffer underflow due to lack of check for negative indices values when 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.com/company/product-security/bulletins/august-2021-bulletin	H-QUA-MDM9-170921/584
Integer Underflow (Wrap or Wraparound)	08-Sep-21	10	Integer underflow can occur due to improper handling of incoming RTCP packets in Snapdragon Auto, Snapdragon Compute,	https://www.qualcomm.com/company/product-security/bull	H-QUA-MDM9-170921/585

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-2021-1920**	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 Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1972**	https://www.qualcomm.com/company/product-security/bulletins/august-2021-bulletin	H-QUA-MDM9-170921/586
mdm9230					
Out-of-bounds Write	08-Sep-21	10	Possible buffer underflow due to lack of check for negative indices values when 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.com/company/product-security/bulletins/august-2021-bulletin	H-QUA-MDM9-170921/587
Integer Underflow	08-Sep-21	10	Integer underflow can occur due to improper handling of	https://www.qualcomm.co	H-QUA-MDM9-

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
(Wrap or Wraparound)			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/bulletins/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 Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1972**	https://www.qualcomm.com/company/product-security/bulletins/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.com/company/product-security/bulletins/august-2021-bulletin	H-QUA-MDM9-170921/590

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.com/company/product-security/bulletins/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.com/company/product-security/bulletins/august-2021-bulletin	H-QUA-MDM9-170921/592
Integer Underflow (Wrap or Wraparound)	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.com/company/product-security/bulletins/august-2021-bulletin	H-QUA-MDM9-170921/593

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Wearables **CVE ID : CVE-2021-1919**		
Integer Underflow (Wrap or Wraparound)	08-Sep-21	10	Integer underflow can occur due to improper 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.com/company/product-security/bulletins/august-2021-bulletin	H-QUA-MDM9-170921/594
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	08-Sep-21	10	Possible buffer overflow due to 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 Networking **CVE ID : CVE-2021-1972**	https://www.qualcomm.com/company/product-security/bulletins/august-2021-bulletin	H-QUA-MDM9-170921/595
mdm9310					
Out-of-bounds Write	08-Sep-21	10	Possible buffer underflow 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.com/company/product-security/bulletins/august-2021-bulletin	H-QUA-MDM9-170921/596

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 Wraparound)	08-Sep-21	10	Integer underflow can occur due to improper 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.com/company/product-security/bulletins/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 Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1972**	https://www.qualcomm.com/company/product-security/bulletins/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.com/company/product-security/bull	H-QUA-MDM9-170921/599

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 Wraparound)	08-Sep-21	10	Integer underflow can occur due to improper 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.com/company/product-security/bulletins/august-2021-bulletin	H-QUA-MDM9-170921/600
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	08-Sep-21	10	Possible buffer overflow due to 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 Networking **CVE ID : CVE-2021-1972**	https://www.qualcomm.com/company/product-security/bulletins/august-2021-bulletin	H-QUA-MDM9-170921/601
mdm9607					
Exposure of Resource to	08-Sep-21	2.1	Child process can leak information from parent	https://www.qualcomm.co	H-QUA-MDM9-

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/bulletins/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.com/company/product-security/bulletins/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.com/company/product-security/bulletins/august-2021-bulletin	H-QUA-MDM9-170921/604

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Integer Underflow (Wrap or Wraparound)	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.com/company/product-security/bulletins/august-2021-bulletin	H-QUA-MDM9-170921/605
Integer Underflow (Wrap or Wraparound)	08-Sep-21	10	Integer underflow can occur due to improper 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.com/company/product-security/bulletins/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 Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking	https://www.qualcomm.com/company/product-security/bulletins/august-2021-bulletin	H-QUA-MDM9-170921/607

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.com/company/product-security/bulletins/august-2021-bulletin	H-QUA-MDM9-170921/608
Integer Underflow (Wrap or Wraparound)	08-Sep-21	10	Integer underflow can occur due to improper 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.com/company/product-security/bulletins/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.com/company/product-security/bulletins/august-2021-bulletin	H-QUA-MDM9-170921/610

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.com/company/product-security/bulletins/august-2021-bulletin	H-QUA-MDM9-170921/611
Integer Underflow (Wrap or Wraparound)	08-Sep-21	10	Integer underflow can occur due to improper 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.com/company/product-security/bulletins/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.com/company/product-security/bulletins/august-2021-bulletin	H-QUA-MDM9-170921/613

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					
Out-of-bounds Write	08-Sep-21	10	Possible buffer underflow due to lack of check for negative indices values when 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.com/company/product-security/bulletins/august-2021-bulletin	H-QUA-MDM9-170921/614
Integer Underflow (Wrap or Wraparound)	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.com/company/product-security/bulletins/august-2021-bulletin	H-QUA-MDM9-170921/615
Integer Underflow (Wrap or Wraparound)	08-Sep-21	10	Integer underflow can occur due to improper handling of incoming RTCP packets in Snapdragon Auto, Snapdragon Compute,	https://www.qualcomm.com/company/product-security/bull	H-QUA-MDM9-170921/616

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-2021-1920**	etins/august-2021-bulletin	
mdm9626					
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.com/company/product-security/bulletins/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 Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1972**	https://www.qualcomm.com/company/product-security/bulletins/august-2021-bulletin	H-QUA-MDM9-170921/618
mdm9628					

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.com/company/product-security/bulletins/august-2021-bulletin	H-QUA-MDM9-170921/619
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.com/company/product-security/bulletins/august-2021-bulletin	H-QUA-MDM9-170921/620
Out-of-bounds Write	08-Sep-21	10	Possible buffer underflow due to lack of check for negative indices values when 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.com/company/product-security/bulletins/august-2021-bulletin	H-QUA-MDM9-170921/621

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2021-1916		
Integer Underflow (Wrap or Wraparound)	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.com/company/product-security/bulletins/august-2021-bulletin	H-QUA-MDM9-170921/622
Integer Underflow (Wrap or Wraparound)	08-Sep-21	10	Integer underflow can occur due to improper 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.com/company/product-security/bulletins/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 Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and	https://www.qualcomm.com/company/product-security/bulletins/august-2021-bulletin	H-QUA-MDM9-170921/624

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Networking **CVE ID : CVE-2021-1972**		
mdm9630					
Out-of-bounds Write	08-Sep-21	10	Possible buffer underflow due to lack of check for negative indices values when 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.com/company/product-security/bulletins/august-2021-bulletin	H-QUA-MDM9-170921/625
Integer Underflow (Wrap or Wraparound)	08-Sep-21	10	Integer underflow can occur due to improper 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.com/company/product-security/bulletins/august-2021-bulletin	H-QUA-MDM9-170921/626
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	08-Sep-21	10	Possible buffer overflow due to 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.com/company/product-security/bulletins/august-2021-bulletin	H-QUA-MDM9-170921/627

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.com/company/product-security/bulletins/august-2021-bulletin	H-QUA-MDM9-170921/628
Integer Underflow (Wrap or Wraparound)	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.com/company/product-security/bulletins/august-2021-bulletin	H-QUA-MDM9-170921/629
Integer Underflow (Wrap or Wraparound)	08-Sep-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.com/company/product-security/bulletins/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.com/company/product-security/bulletins/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.com/company/product-security/bulletins/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.com/company/product-security/bull	H-QUA-MDM9-170921/633

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 Wraparound)	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.com/company/product-security/bulletins/august-2021-bulletin	H-QUA-MDM9-170921/634
Integer Underflow (Wrap or Wraparound)	08-Sep-21	10	Integer underflow can occur due to improper 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.com/company/product-security/bulletins/august-2021-bulletin	H-QUA-MDM9-170921/635
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.com/company/product-security/bulletins/august-	H-QUA-MDM9-170921/636

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					
Out-of-bounds Write	08-Sep-21	10	Possible buffer underflow due to lack of check for negative indices values when 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.com/company/product-security/bulletins/august-2021-bulletin	H-QUA-MDM9-170921/637
Integer Underflow (Wrap or Wraparound)	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.com/company/product-security/bulletins/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.com/company/	H-QUA-MDM9-170921/639

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Wraparound)			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/bulletins/august-2021-bulletin	
mdm9650					
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.com/company/product-security/bulletins/august-2021-bulletin	H-QUA-MDM9-170921/640
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.com/company/product-security/bulletins/august-2021-bulletin	H-QUA-MDM9-170921/641
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.com/company/product-security/bulletins/august-2021-bulletin	MDM9-170921/642
Integer Underflow (Wrap or Wraparound)	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.com/company/product-security/bulletins/august-2021-bulletin	H-QUA-MDM9-170921/643
Integer Underflow (Wrap or Wraparound)	08-Sep-21	10	Integer underflow can occur due to improper 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.com/company/product-security/bulletins/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-

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 Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1972**	m/company/product-security/bulletins/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.com/company/product-security/bulletins/august-2021-bulletin	H-QUA-MDM9-170921/646
Integer Underflow (Wrap or Wraparound)	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.com/company/product-security/bulletins/august-2021-bulletin	H-QUA-MDM9-170921/647

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2021-1919		
Integer Underflow (Wrap or Wraparound)	08-Sep-21	10	Integer underflow can occur due to improper 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.com/company/product-security/bulletins/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.com/company/product-security/bulletins/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.com/company/product-security/bulletins/august-2021-bulletin	H-QUA-MSM8-170921/650

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Wearables **CVE ID : CVE-2021-1916**		
Integer Underflow (Wrap or Wraparound)	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.com/company/product-security/bulletins/august-2021-bulletin	H-QUA-MSM8-170921/651
Integer Underflow (Wrap or Wraparound)	08-Sep-21	10	Integer underflow can occur due to improper 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.com/company/product-security/bulletins/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.com/company/product-security/bulletins/august-2021-bulletin	H-QUA-MSM8-170921/653

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 **CVE ID : CVE-2021-1916**	https://www.qualcomm.com/company/product-security/bulletins/august-2021-bulletin	H-QUA-MSM8-170921/654
Integer Underflow (Wrap or Wraparound)	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.com/company/product-security/bulletins/august-2021-bulletin	H-QUA-MSM8-170921/655
Integer Underflow (Wrap or Wraparound)	08-Sep-21	10	Integer underflow can occur due to improper 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.com/company/product-security/bulletins/august-2021-bulletin	H-QUA-MSM8-170921/656

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2021-1920		
msm8209					
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.com/company/product-security/bulletins/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.com/company/product-security/bulletins/august-2021-bulletin	H-QUA-MSM8-170921/658
Integer Underflow (Wrap or Wraparound)	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.com/company/product-security/bulletins/august-2021-bulletin	H-QUA-MSM8-170921/659

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Wearables **CVE ID : CVE-2021-1919**		
Integer Underflow (Wrap or Wraparound)	08-Sep-21	10	Integer underflow can occur due to improper 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.com/company/product-security/bulletins/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 **CVE ID : CVE-2021-1914**	https://www.qualcomm.com/company/product-security/bulletins/august-2021-bulletin	H-QUA-MSM8-170921/661
Out-of-bounds Write	08-Sep-21	10	Possible buffer underflow due to lack of check for 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.com/company/product-security/bulletins/august-2021-bulletin	H-QUA-MSM8-170921/662

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Voice & Music, Snapdragon Wearables **CVE ID : CVE-2021-1916**		
Integer Underflow (Wrap or Wraparound)	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.com/company/product-security/bulletins/august-2021-bulletin	H-QUA-MSM8-170921/663
Integer Underflow (Wrap or Wraparound)	08-Sep-21	10	Integer underflow can occur due to improper 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.com/company/product-security/bulletins/august-2021-bulletin	H-QUA-MSM8-170921/664
msm8909w					
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.com/company/product-security/bulletins/august-2021-bulletin	H-QUA-MSM8-170921/665

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.com/company/product-security/bulletins/august-2021-bulletin	H-QUA-MSM8-170921/666
Out-of-bounds Write	08-Sep-21	10	Possible buffer underflow due to lack of check for negative indices values when 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.com/company/product-security/bulletins/august-2021-bulletin	H-QUA-MSM8-170921/667
Integer Underflow (Wrap or Wraparound)	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.com/company/product-security/bulletins/august-2021-bulletin	H-QUA-MSM8-170921/668

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 Wraparound)	08-Sep-21	10	Integer underflow can occur due to improper 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.com/company/product-security/bulletins/august-2021-bulletin	H-QUA-MSM8-170921/669
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	08-Sep-21	10	Possible buffer overflow due to 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 Networking **CVE ID : CVE-2021-1972**	https://www.qualcomm.com/company/product-security/bulletins/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.com/company/product-security/bulletins/august-	H-QUA-MSM8-170921/671

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	
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.com/company/product-security/bulletins/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.com/company/product-security/bulletins/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.com/company/product-	H-QUA-MSM8-170921/674

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/bulletins/august-2021-bulletin	
Integer Underflow (Wrap or Wraparound)	08-Sep-21	10	Integer underflow can occur due to improper 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.com/company/product-security/bulletins/august-2021-bulletin	H-QUA-MSM8-170921/675
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	08-Sep-21	10	Possible buffer overflow due to 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 Networking **CVE ID : CVE-2021-1972**	https://www.qualcomm.com/company/product-security/bulletins/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-

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/bulletins/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.com/company/product-security/bulletins/august-2021-bulletin	H-QUA-MSM8-170921/678
Integer Underflow (Wrap or Wraparound)	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.com/company/product-security/bulletins/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-

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
(Wrap or Wraparound)			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/bulletins/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.com/company/product-security/bulletins/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.com/company/product-security/bulletins/august-2021-bulletin	H-QUA-MSM8-170921/682
Integer	08-Sep-21	10	Integer underflow can occur	https://www.	H-QUA-

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Underflow (Wrap or Wraparound)			when 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.com/company/product-security/bulletins/august-2021-bulletin	MSM8-170921/683
Integer Underflow (Wrap or Wraparound)	08-Sep-21	10	Integer underflow can occur due to improper 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.com/company/product-security/bulletins/august-2021-bulletin	H-QUA-MSM8-170921/684
msm8940					
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.com/company/product-security/bulletins/august-2021-bulletin	H-QUA-MSM8-170921/685
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.com/company/product-security/bulletins/august-2021-bulletin	MSM8-170921/686
Integer Underflow (Wrap or Wraparound)	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.com/company/product-security/bulletins/august-2021-bulletin	H-QUA-MSM8-170921/687
Integer Underflow (Wrap or Wraparound)	08-Sep-21	10	Integer underflow can occur due to improper 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.com/company/product-security/bulletins/august-2021-bulletin	H-QUA-MSM8-170921/688
msm8953					
Exposure of	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 Voice & Music, Snapdragon Wearables **CVE ID : CVE-2021-1904**	qualcomm.com/company/product-security/bulletins/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.com/company/product-security/bulletins/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.com/company/product-security/bulletins/august-2021-bulletin	H-QUA-MSM8-170921/691

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2021-1916		
Integer Underflow (Wrap or Wraparound)	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.com/company/product-security/bulletins/august-2021-bulletin	H-QUA-MSM8-170921/692
Integer Underflow (Wrap or Wraparound)	08-Sep-21	10	Integer underflow can occur due to improper 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.com/company/product-security/bulletins/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 Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and	https://www.qualcomm.com/company/product-security/bulletins/august-2021-bulletin	H-QUA-MSM8-170921/694

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.com/company/product-security/bulletins/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.com/company/product-security/bulletins/august-2021-bulletin	H-QUA-MSM8-170921/696
Integer Underflow (Wrap or Wraparound)	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.com/company/product-security/bulletins/august-2021-bulletin	H-QUA-MSM8-170921/697

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Voice & Music, Snapdragon Wearables **CVE ID : CVE-2021-1919**		
Integer Underflow (Wrap or Wraparound)	08-Sep-21	10	Integer underflow can occur due to improper 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.com/company/product-security/bulletins/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.com/company/product-security/bulletins/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.com/company/product-security/bulletins/august-2021-bulletin	H-QUA-MSM8-170921/700

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 Wraparound)	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.com/company/product-security/bulletins/august-2021-bulletin	H-QUA-MSM8-170921/701
Integer Underflow (Wrap or Wraparound)	08-Sep-21	10	Integer underflow can occur due to improper 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.com/company/product-security/bulletins/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.com/company/product-security/bulletins/august-2021-bulletin	H-QUA-MSM8-170921/703

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 **CVE ID : CVE-2021-1914**	https://www.qualcomm.com/company/product-security/bulletins/august-2021-bulletin	H-QUA-MSM8-170921/704
Out-of-bounds Write	08-Sep-21	10	Possible buffer underflow due to lack of check for negative indices values when 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.com/company/product-security/bulletins/august-2021-bulletin	H-QUA-MSM8-170921/705
Integer Underflow (Wrap or Wraparound)	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.com/company/product-security/bulletins/august-2021-bulletin	H-QUA-MSM8-170921/706

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 Wraparound)	08-Sep-21	10	Integer underflow can occur due to improper 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.com/company/product-security/bulletins/august-2021-bulletin	H-QUA-MSM8-170921/707
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.com/company/product-security/bulletins/august-2021-bulletin	H-QUA-MSM8-170921/708
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	08-Sep-21	10	Possible buffer overflow due to 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.com/company/product-security/bulletins/august-2021-bulletin	H-QUA-MSM8-170921/709

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1972**		
pmp8074					
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.com/company/product-security/bulletins/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 Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1972**	https://www.qualcomm.com/company/product-security/bulletins/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.com/company/	H-QUA-QCA1-170921/712

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/bulletins/august-2021-bulletin	
Integer Underflow (Wrap or Wraparound)	08-Sep-21	10	Integer underflow can occur due to improper 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.com/company/product-security/bulletins/august-2021-bulletin	H-QUA-QCA1-170921/713
qca4004					
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.com/company/product-security/bulletins/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/bulletins/august-2021-bulletin	
Integer Underflow (Wrap or Wraparound)	08-Sep-21	10	Integer underflow can occur due to improper 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.com/company/product-security/bulletins/august-2021-bulletin	H-QUA-QCA4-170921/716
qca4020					
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.com/company/product-security/bulletins/august-2021-bulletin	H-QUA-QCA4-170921/717

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 Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1972**	https://www.qualcomm.com/company/product-security/bulletins/august-2021-bulletin	H-QUA-QCA4-170921/718
qca4024					
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.com/company/product-security/bulletins/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.com/company/product-security/bulletins/august-2021-bulletin	H-QUA-QCA4-170921/720

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1972**		
qca6174					
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.com/company/product-security/bulletins/august-2021-bulletin	H-QUA-QCA6-170921/721
Out-of-bounds Write	08-Sep-21	10	Possible buffer underflow due to lack of check for negative indices values when 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.com/company/product-security/bulletins/august-2021-bulletin	H-QUA-QCA6-170921/722
Integer Underflow (Wrap or Wraparound)	08-Sep-21	10	Integer underflow can occur due to improper handling of incoming RTCP packets in Snapdragon Auto, Snapdragon Compute,	https://www.qualcomm.com/company/product-security/bull	H-QUA-QCA6-170921/723

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-2021-1920**	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 Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1972**	https://www.qualcomm.com/company/product-security/bulletins/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 Voice & Music, Snapdragon Wearables **CVE ID : CVE-2021-1904**	https://www.qualcomm.com/company/product-security/bulletins/august-2021-bulletin	H-QUA-QCA6-170921/725
Loop with	08-Sep-21	5	Loop with unreachable exit	https://www.	H-QUA-QCA6-

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.com/company/product-security/bulletins/august-2021-bulletin	170921/726
Out-of-bounds Write	08-Sep-21	10	Possible buffer underflow due to lack of check for negative indices values when 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.com/company/product-security/bulletins/august-2021-bulletin	H-QUA-QCA6-170921/727
Integer Underflow (Wrap or Wraparound)	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.com/company/product-security/bulletins/august-2021-bulletin	H-QUA-QCA6-170921/728
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 Wraparound)			due to improper 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.com/company/product-security/bulletins/august-2021-bulletin	170921/729
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.com/company/product-security/bulletins/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 Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1972**	https://www.qualcomm.com/company/product-security/bulletins/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 Voice & Music, Snapdragon Wearables **CVE ID : CVE-2021-1904**	qualcomm.com/company/product-security/bulletins/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.com/company/product-security/bulletins/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.com/company/product-security/bulletins/august-2021-bulletin	H-QUA-QCA6-170921/734

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2021-1916		
Integer Underflow (Wrap or Wraparound)	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.com/company/product-security/bulletins/august-2021-bulletin	H-QUA-QCA6-170921/735
Integer Underflow (Wrap or Wraparound)	08-Sep-21	10	Integer underflow can occur due to improper 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.com/company/product-security/bulletins/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.com/company/product-security/bulletins/august-2021-bulletin	H-QUA-QCA6-170921/737

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 Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1972**	https://www.qualcomm.com/company/product-security/bulletins/august-2021-bulletin	H-QUA-QCA6-170921/738
qca6320					
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.com/company/product-security/bulletins/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.com/company/product-security/bulletins/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 **CVE ID : CVE-2021-1916**	https://www.qualcomm.com/company/product-security/bulletins/august-2021-bulletin	H-QUA-QCA6-170921/741
Integer Underflow (Wrap or Wraparound)	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.com/company/product-security/bulletins/august-2021-bulletin	H-QUA-QCA6-170921/742
Integer Underflow (Wrap or Wraparound)	08-Sep-21	10	Integer underflow can occur 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.com/company/product-security/bulletins/august-2021-bulletin	H-QUA-QCA6-170921/743

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.com/company/product-security/bulletins/august-2021-bulletin	H-QUA-QCA6-170921/744
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	08-Sep-21	10	Possible buffer overflow due to 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 Networking **CVE ID : CVE-2021-1972**	https://www.qualcomm.com/company/product-security/bulletins/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.com/company/product-security/bulletins/august-	H-QUA-QCA6-170921/746

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	
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.com/company/product-security/bulletins/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.com/company/product-security/bulletins/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.com/company/product-	H-QUA-QCA6-170921/749

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/bulletins/august-2021-bulletin	
Integer Underflow (Wrap or Wraparound)	08-Sep-21	10	Integer underflow can occur due to improper 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.com/company/product-security/bulletins/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.com/company/product-security/bulletins/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.com/company/product-security/bull	H-QUA-QCA6-170921/752

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					
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.com/company/product-security/bulletins/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.com/company/product-security/bulletins/august-2021-bulletin	H-QUA-QCA6-170921/754

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.com/company/product-security/bulletins/august-2021-bulletin	H-QUA-QCA6-170921/755
Integer Underflow (Wrap or Wraparound)	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.com/company/product-security/bulletins/august-2021-bulletin	H-QUA-QCA6-170921/756
Integer Underflow (Wrap or Wraparound)	08-Sep-21	10	Integer underflow can occur due to improper 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.com/company/product-security/bulletins/august-2021-bulletin	H-QUA-QCA6-170921/757
Incorrect	08-Sep-21	4.6	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.com/company/product-security/bulletins/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.com/company/product-security/bulletins/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.com/company/product-security/bulletins/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.com/company/product-security/bulletins/august-2021-bulletin	H-QUA-QCA6-170921/761

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 Voice & Music, Snapdragon Wearables **CVE ID : CVE-2021-1904**	https://www.qualcomm.com/company/product-security/bulletins/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.com/company/product-security/bulletins/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.com/company/product-	H-QUA-QCA6-170921/764

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/bulletins/august-2021-bulletin	
Integer Underflow (Wrap or Wraparound)	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.com/company/product-security/bulletins/august-2021-bulletin	H-QUA-QCA6-170921/765
Integer Underflow (Wrap or Wraparound)	08-Sep-21	10	Integer underflow can occur due to improper 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.com/company/product-security/bulletins/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.com/company/product-security/bull	H-QUA-QCA6-170921/767

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.com/company/product-security/bulletins/august-2021-bulletin	H-QUA-QCA6-170921/768
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.com/company/product-security/bulletins/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 Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and	https://www.qualcomm.com/company/product-security/bulletins/august-2021-bulletin	H-QUA-QCA6-170921/770

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 Voice & Music, Snapdragon Wearables **CVE ID : CVE-2021-1904**	https://www.qualcomm.com/company/product-security/bulletins/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.com/company/product-security/bulletins/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.com/company/product-security/bulletins/august-2021-bulletin	H-QUA-QCA6-170921/773

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 Wraparound)	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.com/company/product-security/bulletins/august-2021-bulletin	H-QUA-QCA6-170921/774
Integer Underflow (Wrap or Wraparound)	08-Sep-21	10	Integer underflow can occur due to improper 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.com/company/product-security/bulletins/august-2021-bulletin	H-QUA-QCA6-170921/775
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.com/company/product-security/bulletins/august-2021-bulletin	H-QUA-QCA6-170921/776

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.com/company/product-security/bulletins/august-2021-bulletin	H-QUA-QCA6-170921/777
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.com/company/product-security/bulletins/august-2021-bulletin	H-QUA-QCA6-170921/778
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	08-Sep-21	10	Possible buffer overflow due to 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 Networking **CVE ID : CVE-2021-1972**	https://www.qualcomm.com/company/product-security/bulletins/august-2021-bulletin	H-QUA-QCA6-170921/779
qca6421					
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 Voice & Music, Snapdragon Wearables **CVE ID : CVE-2021-1904**	qualcomm.com/company/product-security/bulletins/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.com/company/product-security/bulletins/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.com/company/product-security/bulletins/august-2021-bulletin	H-QUA-QCA6-170921/782

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2021-1916		
Integer Underflow (Wrap or Wraparound)	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.com/company/product-security/bulletins/august-2021-bulletin	H-QUA-QCA6-170921/783
Integer Underflow (Wrap or Wraparound)	08-Sep-21	10	Integer underflow can occur due to improper 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.com/company/product-security/bulletins/august-2021-bulletin	H-QUA-QCA6-170921/784
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.com/company/product-security/bulletins/august-2021-bulletin	H-QUA-QCA6-170921/785
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.com/company/product-	H-QUA-QCA6-170921/786

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/bulletins/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.com/company/product-security/bulletins/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 Mobile, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1972**	https://www.qualcomm.com/company/product-security/bulletins/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.com/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.com/company/product-security/bulletins/august-2021-bulletin	H-QUA-QCA6-170921/790
Out-of-bounds Write	08-Sep-21	10	Possible buffer underflow due to lack of check for negative indices values when 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.com/company/product-security/bulletins/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.com/company/	H-QUA-QCA6-170921/792

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Wraparound)			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/bulletins/august-2021-bulletin	
Integer Underflow (Wrap or Wraparound)	08-Sep-21	10	Integer underflow can occur due to improper 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.com/company/product-security/bulletins/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.com/company/product-security/bulletins/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.com/company/product-security/bulletins/august-2021-bulletin	H-QUA-QCA6-170921/795

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.com/company/product-security/bulletins/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 Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1972**	https://www.qualcomm.com/company/product-security/bulletins/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.com/company/product-security/bulletins/august-2021-bulletin	H-QUA-QCA6-170921/798

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 Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1972**	https://www.qualcomm.com/company/product-security/bulletins/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 Voice & Music, Snapdragon Wearables **CVE ID : CVE-2021-1904**	https://www.qualcomm.com/company/product-security/bulletins/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.com/company/product-	H-QUA-QCA6-170921/801

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/bulletins/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.com/company/product-security/bulletins/august-2021-bulletin	H-QUA-QCA6-170921/802
Integer Underflow (Wrap or Wraparound)	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.com/company/product-security/bulletins/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.com/company/product-	H-QUA-QCA6-170921/804

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/bulletins/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.com/company/product-security/bulletins/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.com/company/product-security/bulletins/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.com/company/product-security/bulletins/august-2021-bulletin	H-QUA-QCA6-170921/807

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 Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1972**	https://www.qualcomm.com/company/product-security/bulletins/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.com/company/product-security/bulletins/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.com/company/product-security/bulletins/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 **CVE ID : CVE-2021-1916**	https://www.qualcomm.com/company/product-security/bulletins/august-2021-bulletin	H-QUA-QCA6-170921/811
Integer Underflow (Wrap or Wraparound)	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.com/company/product-security/bulletins/august-2021-bulletin	H-QUA-QCA6-170921/812
Integer Underflow (Wrap or Wraparound)	08-Sep-21	10	Integer underflow can occur 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.com/company/product-security/bulletins/august-2021-bulletin	H-QUA-QCA6-170921/813

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.com/company/product-security/bulletins/august-2021-bulletin	H-QUA-QCA6-170921/814
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.com/company/product-security/bulletins/august-2021-bulletin	H-QUA-QCA6-170921/815
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.com/company/product-security/bulletins/august-2021-bulletin	H-QUA-QCA6-170921/816
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.com/company/product-security/bull	H-QUA-QCA6-170921/817

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					
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.com/company/product-security/bulletins/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.com/company/product-security/bulletins/august-2021-bulletin	H-QUA-QCA6-170921/819

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.com/company/product-security/bulletins/august-2021-bulletin	H-QUA-QCA6-170921/820
Integer Underflow (Wrap or Wraparound)	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.com/company/product-security/bulletins/august-2021-bulletin	H-QUA-QCA6-170921/821
Integer Underflow (Wrap or Wraparound)	08-Sep-21	10	Integer underflow can occur due to improper 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.com/company/product-security/bulletins/august-2021-bulletin	H-QUA-QCA6-170921/822
Incorrect	08-Sep-21	4.6	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.com/company/product-security/bulletins/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.com/company/product-security/bulletins/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.com/company/product-security/bulletins/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.com/company/product-security/bulletins/august-2021-bulletin	H-QUA-QCA6-170921/826

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**		
qca6438					
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.com/company/product-security/bulletins/august-2021-bulletin	H-QUA-QCA6-170921/827
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	08-Sep-21	10	Possible buffer overflow due to 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 Networking **CVE ID : CVE-2021-1972**	https://www.qualcomm.com/company/product-security/bulletins/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-

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/bulletins/august-2021-bulletin	170921/829
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	08-Sep-21	10	Possible buffer overflow due to 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 Networking **CVE ID : CVE-2021-1972**	https://www.qualcomm.com/company/product-security/bulletins/august-2021-bulletin	H-QUA-QCA6-170921/830
qca6564a					
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.com/company/product-security/bulletins/august-2021-bulletin	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.com/company/product-security/bulletins/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.com/company/product-security/bulletins/august-2021-bulletin	H-QUA-QCA6-170921/833
Integer Underflow (Wrap or Wraparound)	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.com/company/product-security/bulletins/august-2021-bulletin	H-QUA-QCA6-170921/834

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Voice & Music, Snapdragon Wearables **CVE ID : CVE-2021-1919**		
Integer Underflow (Wrap or Wraparound)	08-Sep-21	10	Integer underflow can occur due to improper 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.com/company/product-security/bulletins/august-2021-bulletin	H-QUA-QCA6-170921/835
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.com/company/product-security/bulletins/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 Voice & Music, Snapdragon Wearables, Snapdragon Wired	https://www.qualcomm.com/company/product-security/bulletins/august-2021-bulletin	H-QUA-QCA6-170921/837

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Infrastructure and Networking **CVE ID : CVE-2021-1972**		
qca6564au					
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.com/company/product-security/bulletins/august-2021-bulletin	H-QUA-QCA6-170921/838
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.com/company/product-security/bulletins/august-2021-bulletin	H-QUA-QCA6-170921/839
Out-of-bounds Write	08-Sep-21	10	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.com/company/product-security/bulletins/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 Wraparound)	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.com/company/product-security/bulletins/august-2021-bulletin	H-QUA-QCA6-170921/841
Integer Underflow (Wrap or Wraparound)	08-Sep-21	10	Integer underflow can occur due to improper 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.com/company/product-security/bulletins/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.com/company/product-security/bulletins/august-2021-bulletin	H-QUA-QCA6-170921/843

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.com/company/product-security/bulletins/august-2021-bulletin	H-QUA-QCA6-170921/844
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	08-Sep-21	10	Possible buffer overflow due to 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 Networking **CVE ID : CVE-2021-1972**	https://www.qualcomm.com/company/product-security/bulletins/august-2021-bulletin	H-QUA-QCA6-170921/845
qca6574					
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.com/company/product-security/bulletins/august-2021-bulletin	H-QUA-QCA6-170921/846

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 **CVE ID : CVE-2021-1914**	https://www.qualcomm.com/company/product-security/bulletins/august-2021-bulletin	H-QUA-QCA6-170921/847
Out-of-bounds Write	08-Sep-21	10	Possible buffer underflow due to lack of check for negative indices values when 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.com/company/product-security/bulletins/august-2021-bulletin	H-QUA-QCA6-170921/848
Integer Underflow (Wrap or Wraparound)	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.com/company/product-security/bulletins/august-2021-bulletin	H-QUA-QCA6-170921/849

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 Wraparound)	08-Sep-21	10	Integer underflow can occur due to improper 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.com/company/product-security/bulletins/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.com/company/product-security/bulletins/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.com/company/product-security/bulletins/august-2021-bulletin	H-QUA-QCA6-170921/852
Buffer Copy without	08-Sep-21	10	Possible buffer overflow due to improper validation of	https://www.qualcomm.co	H-QUA-QCA6-

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 Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1972**	m/company/product-security/bulletins/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.com/company/product-security/bulletins/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.com/company/product-security/bulletins/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 **CVE ID : CVE-2021-1916**	https://www.qualcomm.com/company/product-security/bulletins/august-2021-bulletin	H-QUA-QCA6-170921/856
Integer Underflow (Wrap or Wraparound)	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.com/company/product-security/bulletins/august-2021-bulletin	H-QUA-QCA6-170921/857
Integer Underflow (Wrap or Wraparound)	08-Sep-21	10	Integer underflow can occur due to improper 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.com/company/product-security/bulletins/august-2021-bulletin	H-QUA-QCA6-170921/858

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.com/company/product-security/bulletins/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.com/company/product-security/bulletins/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.com/company/product-security/bulletins/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.com/company/product-security/bulletins/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 **CVE ID : CVE-2021-1972**		
qca6574au					
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.com/company/product-security/bulletins/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.com/company/product-security/bulletins/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/bulletins/august-2021-bulletin	
Integer Underflow (Wrap or Wraparound)	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.com/company/product-security/bulletins/august-2021-bulletin	H-QUA-QCA6-170921/866
Integer Underflow (Wrap or Wraparound)	08-Sep-21	10	Integer underflow can occur due to improper 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.com/company/product-security/bulletins/august-2021-bulletin	H-QUA-QCA6-170921/867
Incorrect Type Conversion	08-Sep-21	4.6	Incorrect pointer argument passed to trusted application TA could result in un-	https://www.qualcomm.com/company/	H-QUA-QCA6-170921/868

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/bulletins/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.com/company/product-security/bulletins/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.com/company/product-security/bulletins/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.com/company/product-security/bulletins/august-2021-bulletin	H-QUA-QCA6-170921/871

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 Voice & Music, Snapdragon Wearables **CVE ID : CVE-2021-1904**	https://www.qualcomm.com/company/product-security/bulletins/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.com/company/product-security/bulletins/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.com/company/product-security/bulletins/august-	H-QUA-QCA6-170921/874

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-2021-1916**	2021-bulletin	
Integer Underflow (Wrap or Wraparound)	08-Sep-21	10	Integer underflow can occur due to improper 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.com/company/product-security/bulletins/august-2021-bulletin	H-QUA-QCA6-170921/875
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	08-Sep-21	10	Possible buffer overflow due to 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 Networking **CVE ID : CVE-2021-1972**	https://www.qualcomm.com/company/product-security/bulletins/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.com/company/	H-QUA-QCA6-170921/877

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/bulletins/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.com/company/product-security/bulletins/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.com/company/product-security/bulletins/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 Wraparound)			when 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.com/company/product-security/bulletins/august-2021-bulletin	170921/880
Integer Underflow (Wrap or Wraparound)	08-Sep-21	10	Integer underflow can occur due to improper 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.com/company/product-security/bulletins/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.com/company/product-security/bulletins/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.com/company/product-security/bull	H-QUA-QCA6-170921/883

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					
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.com/company/product-security/bulletins/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.com/company/product-security/bulletins/august-2021-bulletin	H-QUA-QCA6-170921/885
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.com/company/product-	H-QUA-QCA6-170921/886

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/bulletins/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 Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1972**	https://www.qualcomm.com/company/product-security/bulletins/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, Snapdragon Wearables **CVE ID : CVE-2021-1904**	https://www.qualcomm.com/company/product-security/bulletins/august-2021-bulletin	H-QUA-QCA6-170921/888
Loop with	08-Sep-21	5	Loop with unreachable exit	https://www.	H-QUA-QCA6-

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.com/company/product-security/bulletins/august-2021-bulletin	170921/889
Out-of-bounds Write	08-Sep-21	10	Possible buffer underflow due to lack of check for negative indices values when 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.com/company/product-security/bulletins/august-2021-bulletin	H-QUA-QCA6-170921/890
Integer Underflow (Wrap or Wraparound)	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.com/company/product-security/bulletins/august-2021-bulletin	H-QUA-QCA6-170921/891
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 Wraparound)			due to improper 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.com/company/product-security/bulletins/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.com/company/product-security/bulletins/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.com/company/product-security/bulletins/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.com/company/product-security/bulletins/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 Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1972**	https://www.qualcomm.com/company/product-security/bulletins/august-2021-bulletin	H-QUA-QCA6-170921/896
qca6694					
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.com/company/product-security/bulletins/august-2021-bulletin	H-QUA-QCA6-170921/897
Out-of-bounds Write	08-Sep-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.com/company/product-security/bulletins/august-	H-QUA-QCA6-170921/898

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-2021-1916**	2021-bulletin	
Integer Underflow (Wrap or Wraparound)	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.com/company/product-security/bulletins/august-2021-bulletin	H-QUA-QCA6-170921/899
Integer Underflow (Wrap or Wraparound)	08-Sep-21	10	Integer underflow can occur due to improper 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.com/company/product-security/bulletins/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.com/company/product-security/bulletins/august-2021-bulletin	H-QUA-QCA6-170921/901

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 Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1972**	https://www.qualcomm.com/company/product-security/bulletins/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.com/company/product-security/bulletins/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.com/company/	H-QUA-QCA6-170921/904

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/bulletins/august-2021-bulletin	
Integer Underflow (Wrap or Wraparound)	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.com/company/product-security/bulletins/august-2021-bulletin	H-QUA-QCA6-170921/905
Integer Underflow (Wrap or Wraparound)	08-Sep-21	10	Integer underflow can occur due to improper 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.com/company/product-security/bulletins/august-2021-bulletin	H-QUA-QCA6-170921/906
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.com/company/	H-QUA-QCA6-170921/907

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/bulletins/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.com/company/product-security/bulletins/august-2021-bulletin	H-QUA-QCA6-170921/908
Out-of-bounds Write	08-Sep-21	10	Possible buffer underflow due to lack of check for negative indices values when 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.com/company/product-security/bulletins/august-2021-bulletin	H-QUA-QCA6-170921/909
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 Wraparound)			when 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.com/company/product-security/bulletins/august-2021-bulletin	170921/910
Integer Underflow (Wrap or Wraparound)	08-Sep-21	10	Integer underflow can occur due to improper 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.com/company/product-security/bulletins/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.com/company/product-security/bulletins/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.com/company/product-security/bulletins/august-	H-QUA-QCA6-170921/913

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wearables **CVE ID : CVE-2021-1929**	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.com/company/product-security/bulletins/august-2021-bulletin	H-QUA-QCA6-170921/914
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	08-Sep-21	10	Possible buffer overflow due to 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 Networking **CVE ID : CVE-2021-1972**	https://www.qualcomm.com/company/product-security/bulletins/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.com/company/product-security/bulletins/august-2021-bulletin	H-QUA-QCA7-170921/916

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 Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1972**	https://www.qualcomm.com/company/product-security/bulletins/august-2021-bulletin	H-QUA-QCA7-170921/917
qca7520					
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	08-Sep-21	10	Possible buffer overflow due to 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 Networking **CVE ID : CVE-2021-1972**	https://www.qualcomm.com/company/product-security/bulletins/august-2021-bulletin	H-QUA-QCA7-170921/918
qca7550					

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 Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1972**	https://www.qualcomm.com/company/product-security/bulletins/august-2021-bulletin	H-QUA-QCA7-170921/919
qca8072					
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.com/company/product-security/bulletins/august-2021-bulletin	H-QUA-QCA8-170921/920
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	08-Sep-21	10	Possible buffer overflow due to 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.com/company/product-security/bulletins/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					
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.com/company/product-security/bulletins/august-2021-bulletin	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 Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1972**	https://www.qualcomm.com/company/product-security/bulletins/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.com/company/	H-QUA-QCA8-170921/924

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/bulletins/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 Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1972**	https://www.qualcomm.com/company/product-security/bulletins/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.com/company/product-security/bulletins/august-2021-bulletin	H-QUA-QCA8-170921/926

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 Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1972**	https://www.qualcomm.com/company/product-security/bulletins/august-2021-bulletin	H-QUA-QCA8-170921/927
qca9367					
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.com/company/product-security/bulletins/august-2021-bulletin	H-QUA-QCA9-170921/928
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.com/company/product-security/bulletins/august-	H-QUA-QCA9-170921/929

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.com/company/product-security/bulletins/august-2021-bulletin	H-QUA-QCA9-170921/930
Integer Underflow (Wrap or Wraparound)	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.com/company/product-security/bulletins/august-2021-bulletin	H-QUA-QCA9-170921/931
Integer Underflow (Wrap or Wraparound)	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.com/company/product-security/bulletins/august-	H-QUA-QCA9-170921/932

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	
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.com/company/product-security/bulletins/august-2021-bulletin	H-QUA-QCA9-170921/933
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	08-Sep-21	10	Possible buffer overflow due to 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 Networking **CVE ID : CVE-2021-1972**	https://www.qualcomm.com/company/product-security/bulletins/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.com/company/	H-QUA-QCA9-170921/935

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/bulletins/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.com/company/product-security/bulletins/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.com/company/product-security/bulletins/august-2021-bulletin	H-QUA-QCA9-170921/937
Integer	08-Sep-21	10	Integer underflow can occur	https://www.	H-QUA-QCA9-

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Underflow (Wrap or Wraparound)			when 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.com/company/product-security/bulletins/august-2021-bulletin	170921/938
Integer Underflow (Wrap or Wraparound)	08-Sep-21	10	Integer underflow can occur due to improper 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.com/company/product-security/bulletins/august-2021-bulletin	H-QUA-QCA9-170921/939
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.com/company/product-security/bulletins/august-2021-bulletin	H-QUA-QCA9-170921/940
Improper Restriction	08-Sep-21	3.6	Possible out of bounds read due to incorrect validation of	https://www.qualcomm.co	H-QUA-QCA9-170921/941

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/bulletins/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 Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1972**	https://www.qualcomm.com/company/product-security/bulletins/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 Voice & Music, Snapdragon Wearables **CVE ID : CVE-2021-1904**	https://www.qualcomm.com/company/product-security/bulletins/august-2021-bulletin	H-QUA-QCA9-170921/943

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.com/company/product-security/bulletins/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.com/company/product-security/bulletins/august-2021-bulletin	H-QUA-QCA9-170921/945
Integer Underflow (Wrap or Wraparound)	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.com/company/product-security/bulletins/august-2021-bulletin	H-QUA-QCA9-170921/946

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Integer Underflow (Wrap or Wraparound)	08-Sep-21	10	Integer underflow can occur due to improper 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.com/company/product-security/bulletins/august-2021-bulletin	H-QUA-QCA9-170921/947
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	08-Sep-21	10	Possible buffer overflow due to 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 Networking **CVE ID : CVE-2021-1972**	https://www.qualcomm.com/company/product-security/bulletins/august-2021-bulletin	H-QUA-QCA9-170921/948
qca9531					
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.com/company/product-security/bulletins/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 Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1972**	https://www.qualcomm.com/company/product-security/bulletins/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.com/company/product-security/bulletins/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.com/company/product-security/bulletins/august-2021-bulletin	H-QUA-QCA9-170921/952

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.com/company/product-security/bulletins/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 Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1972**	https://www.qualcomm.com/company/product-security/bulletins/august-2021-bulletin	H-QUA-QCA9-170921/954
qca9563					

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.com/company/product-security/bulletins/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 Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1972**	https://www.qualcomm.com/company/product-security/bulletins/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.com/company/product-security/bulletins/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 Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1972**	https://www.qualcomm.com/company/product-security/bulletins/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.com/company/product-security/bulletins/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.com/company/product-security/bulletins/august-	H-QUA-QCA9-170921/960

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					
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.com/company/product-security/bulletins/august-2021-bulletin	H-QUA-QCA9-170921/961
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	08-Sep-21	10	Possible buffer overflow due to 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 Networking **CVE ID : CVE-2021-1972**	https://www.qualcomm.com/company/product-security/bulletins/august-2021-bulletin	H-QUA-QCA9-170921/962

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
qca9887					
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.com/company/product-security/bulletins/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 Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1972**	https://www.qualcomm.com/company/product-security/bulletins/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.com/company/product-security/bulletins/august-2021-bulletin	H-QUA-QCA9-170921/965

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 Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1972**	https://www.qualcomm.com/company/product-security/bulletins/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.com/company/product-security/bulletins/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.com/company/product-	H-QUA-QCA9-170921/968

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/bulletins/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.com/company/product-security/bulletins/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 Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and	https://www.qualcomm.com/company/product-security/bulletins/august-2021-bulletin	H-QUA-QCA9-170921/970

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Networking **CVE ID : CVE-2021-1972**		
qca9898					
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.com/company/product-security/bulletins/august-2021-bulletin	H-QUA-QCA9-170921/971
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	08-Sep-21	10	Possible buffer overflow due to 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 Networking **CVE ID : CVE-2021-1972**	https://www.qualcomm.com/company/product-security/bulletins/august-2021-bulletin	H-QUA-QCA9-170921/972
qca9980					
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.com/company/product-security/bulletins/august-	H-QUA-QCA9-170921/973

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1928**	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 Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1972**	https://www.qualcomm.com/company/product-security/bulletins/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.com/company/product-security/bulletins/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 Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1972**	m/company/product-security/bulletins/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 **CVE ID : CVE-2021-1928**	https://www.qualcomm.com/company/product-security/bulletins/august-2021-bulletin	H-QUA-QCA9-170921/977
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	08-Sep-21	10	Possible buffer overflow due to 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	https://www.qualcomm.com/company/product-security/bulletins/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.com/company/product-security/bulletins/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 Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1972**	https://www.qualcomm.com/company/product-security/bulletins/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.com/company/product-security/bull	H-QUA-QCA9-170921/981

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 Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1972**	https://www.qualcomm.com/company/product-security/bulletins/august-2021-bulletin	H-QUA-QCA9-170921/982
qca9988					
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	08-Sep-21	10	Possible buffer overflow due to 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.com/company/product-security/bulletins/august-2021-bulletin	H-QUA-QCA9-170921/983

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 **CVE ID : CVE-2021-1928**	https://www.qualcomm.com/company/product-security/bulletins/august-2021-bulletin	H-QUA-QCA9-170921/984
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	08-Sep-21	10	Possible buffer overflow due to 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 Networking **CVE ID : CVE-2021-1972**	https://www.qualcomm.com/company/product-security/bulletins/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.com/company/product-	H-QUA-QCA9-170921/986

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/bulletins/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 Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1972**	https://www.qualcomm.com/company/product-security/bulletins/august-2021-bulletin	H-QUA-QCA9-170921/987
qca9994					
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.com/company/product-security/bulletins/august-2021-bulletin	H-QUA-QCA9-170921/988

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 Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1972**	https://www.qualcomm.com/company/product-security/bulletins/august-2021-bulletin	H-QUA-QCA9-170921/989
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.com/company/product-security/bulletins/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.com/company/product-security/bulletins/august-2021-bulletin	H-QUA-QCM2-170921/991

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.com/company/product-security/bulletins/august-2021-bulletin	H-QUA-QCM2-170921/992
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.com/company/product-security/bulletins/august-2021-bulletin	H-QUA-QCM2-170921/993
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	08-Sep-21	10	Possible buffer overflow due to 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 Networking **CVE ID : CVE-2021-1972**	https://www.qualcomm.com/company/product-security/bulletins/august-2021-bulletin	H-QUA-QCM2-170921/994
qcm4290					

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.com/company/product-security/bulletins/august-2021-bulletin	H-QUA-QCM4-170921/995
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.com/company/product-security/bulletins/august-2021-bulletin	H-QUA-QCM4-170921/996
Out-of-bounds Write	08-Sep-21	10	Possible buffer underflow due to lack of check for negative indices values when 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.com/company/product-security/bulletins/august-2021-bulletin	H-QUA-QCM4-170921/997

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2021-1916		
Integer Underflow (Wrap or Wraparound)	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.com/company/product-security/bulletins/august-2021-bulletin	H-QUA-QCM4-170921/998
Integer Underflow (Wrap or Wraparound)	08-Sep-21	10	Integer underflow can occur due to improper 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.com/company/product-security/bulletins/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.com/company/product-security/bulletins/august-2021-bulletin	H-QUA-QCM4-170921/1000
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.com/company/product-	H-QUA-QCM4-170921/1001

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/bulletins/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.com/company/product-security/bulletins/august-2021-bulletin	H-QUA-QCM4-170921/1002
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	08-Sep-21	10	Possible buffer overflow due to 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 Networking **CVE ID : CVE-2021-1972**	https://www.qualcomm.com/company/product-security/bulletins/august-2021-bulletin	H-QUA-QCM4-170921/1003
qcm6125					
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.com/company/product-security/bull	H-QUA-QCM6-170921/1004

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.com/company/product-security/bulletins/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.com/company/product-security/bulletins/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.com/company/	H-QUA-QCM6-170921/1007

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Wraparound)			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/bulletins/august-2021-bulletin	
Integer Underflow (Wrap or Wraparound)	08-Sep-21	10	Integer underflow can occur due to improper 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.com/company/product-security/bulletins/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.com/company/product-security/bulletins/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.com/company/product-security/bulletins/august-	H-QUA-QCM6-170921/1010

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 Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1972**	https://www.qualcomm.com/company/product-security/bulletins/august-2021-bulletin	H-QUA-QCM6-170921/1011
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 Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1972**	https://www.qualcomm.com/company/product-security/bulletins/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-

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/bulletins/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 Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1972**	https://www.qualcomm.com/company/product-security/bulletins/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.com/company/product-security/bulletins/august-2021-bulletin	H-QUA-QCN5-170921/1015

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 Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1972**	https://www.qualcomm.com/company/product-security/bulletins/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.com/company/product-security/bulletins/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.com/company/product-security/bulletins/august-2021-bulletin	H-QUA-QCN5-170921/1018

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.com/company/product-security/bulletins/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 Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1972**	https://www.qualcomm.com/company/product-security/bulletins/august-2021-bulletin	H-QUA-QCN5-170921/1020
qcn5054					

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.com/company/product-security/bulletins/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 Mobile, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1972**	https://www.qualcomm.com/company/product-security/bulletins/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 Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon	https://www.qualcomm.com/company/product-security/bulletins/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 Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1972**	https://www.qualcomm.com/company/product-security/bulletins/august-2021-bulletin	H-QUA-QCN5-170921/1024
qcn5121					
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.com/company/product-security/bulletins/august-2021-bulletin	H-QUA-QCN5-170921/1025
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.com/company/product-security/bulletins/august-	H-QUA-QCN5-170921/1026

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					
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.com/company/product-security/bulletins/august-2021-bulletin	H-QUA-QCN5-170921/1027
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	08-Sep-21	10	Possible buffer overflow due to 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 Networking **CVE ID : CVE-2021-1972**	https://www.qualcomm.com/company/product-security/bulletins/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.com/company/product-security/bulletins/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 Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1972**	https://www.qualcomm.com/company/product-security/bulletins/august-2021-bulletin	H-QUA-QCN5-170921/1030
qcn5152					
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.com/company/product-security/bulletins/august-2021-bulletin	H-QUA-QCN5-170921/1031

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 Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1972**	https://www.qualcomm.com/company/product-security/bulletins/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.com/company/product-security/bulletins/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.com/company/product-	H-QUA-QCN5-170921/1034

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/bulletins/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.com/company/product-security/bulletins/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 Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and	https://www.qualcomm.com/company/product-security/bulletins/august-2021-bulletin	H-QUA-QCN5-170921/1036

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.com/company/product-security/bulletins/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 Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1972**	https://www.qualcomm.com/company/product-security/bulletins/august-2021-bulletin	H-QUA-QCN5-170921/1038
qcn5502					
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.com/company/product-security/bulletins/august-	H-QUA-QCN5-170921/1039

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1928**	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 Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1972**	https://www.qualcomm.com/company/product-security/bulletins/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.com/company/product-security/bulletins/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 Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1972**	m/company/product-security/bulletins/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 **CVE ID : CVE-2021-1928**	https://www.qualcomm.com/company/product-security/bulletins/august-2021-bulletin	H-QUA-QCN6-170921/1043
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	08-Sep-21	10	Possible buffer overflow due to 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	https://www.qualcomm.com/company/product-security/bulletins/august-2021-bulletin	H-QUA-QCN6-170921/1044

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Infrastructure and Networking **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.com/company/product-security/bulletins/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 Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1972**	https://www.qualcomm.com/company/product-security/bulletins/august-2021-bulletin	H-QUA-QCN6-170921/1046
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.com/company/product-security/bull	H-QUA-QCN6-170921/1047

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.com/company/product-security/bulletins/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 Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking	https://www.qualcomm.com/company/product-security/bulletins/august-2021-bulletin	H-QUA-QCN9-170921/1049

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 **CVE ID : CVE-2021-1928**	https://www.qualcomm.com/company/product-security/bulletins/august-2021-bulletin	H-QUA-QCN9-170921/1050
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	08-Sep-21	10	Possible buffer overflow due to 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 Networking **CVE ID : CVE-2021-1972**	https://www.qualcomm.com/company/product-security/bulletins/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.com/company/product-security/bulletins/august-2021-bulletin	H-QUA-QCN9-170921/1052

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 Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1972**	https://www.qualcomm.com/company/product-security/bulletins/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.com/company/product-security/bulletins/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.com/company/	H-QUA-QCN9-170921/1055

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/bulletins/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.com/company/product-security/bulletins/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 Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and	https://www.qualcomm.com/company/product-security/bulletins/august-2021-bulletin	H-QUA-QCN9-170921/1057

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Networking **CVE ID : CVE-2021-1972**		
qcn9072					
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.com/company/product-security/bulletins/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 Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1972**	https://www.qualcomm.com/company/product-security/bulletins/august-2021-bulletin	H-QUA-QCN9-170921/1059
qcn9074					
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.com/company/product-security/bulletins/august-	H-QUA-QCN9-170921/1060

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1928**	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 Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1972**	https://www.qualcomm.com/company/product-security/bulletins/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.com/company/product-security/bulletins/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	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 Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1972**	m/company/product-security/bulletins/august-2021-bulletin	
qcs2290					
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.com/company/product-security/bulletins/august-2021-bulletin	H-QUA-QCS2-170921/1064
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://www.qualcomm.com/company/product-security/bulletins/august-2021-bulletin	H-QUA-QCS2-170921/1065
Exposure of	08-Sep-21	2.1	Lack of strict validation of	https://www.	H-QUA-QCS2-

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.com/company/product-security/bulletins/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.com/company/product-security/bulletins/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 Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1972**	https://www.qualcomm.com/company/product-security/bulletins/august-2021-bulletin	H-QUA-QCS2-170921/1068
qcs405					
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

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/bulletins/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 Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1972**	https://www.qualcomm.com/company/product-security/bulletins/august-2021-bulletin	H-QUA-QCS4-170921/1070
qcs410					
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.com/company/product-security/bulletins/august-2021-bulletin	H-QUA-QCS4-170921/1071

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.com/company/product-security/bulletins/august-2021-bulletin	H-QUA-QCS4-170921/1072
Out-of-bounds Write	08-Sep-21	10	Possible buffer underflow due to lack of check for negative indices values when 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.com/company/product-security/bulletins/august-2021-bulletin	H-QUA-QCS4-170921/1073
Integer Underflow (Wrap or Wraparound)	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.com/company/product-security/bulletins/august-2021-bulletin	H-QUA-QCS4-170921/1074

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Voice & Music, Snapdragon Wearables **CVE ID : CVE-2021-1919**		
Integer Underflow (Wrap or Wraparound)	08-Sep-21	10	Integer underflow can occur due to improper 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.com/company/product-security/bulletins/august-2021-bulletin	H-QUA-QCS4-170921/1075
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.com/company/product-security/bulletins/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 Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and	https://www.qualcomm.com/company/product-security/bulletins/august-2021-bulletin	H-QUA-QCS4-170921/1077

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, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2021-1904**	https://www.qualcomm.com/company/product-security/bulletins/august-2021-bulletin	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.com/company/product-security/bulletins/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.com/company/product-security/bulletins/august-2021-bulletin	H-QUA-QCS4-170921/1080

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 Wraparound)	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.com/company/product-security/bulletins/august-2021-bulletin	H-QUA-QCS4-170921/1081
Integer Underflow (Wrap or Wraparound)	08-Sep-21	10	Integer underflow can occur due to improper 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.com/company/product-security/bulletins/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.com/company/product-security/bulletins/august-2021-bulletin	H-QUA-QCS4-170921/1083

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.com/company/product-security/bulletins/august-2021-bulletin	H-QUA-QCS4-170921/1084
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.com/company/product-security/bulletins/august-2021-bulletin	H-QUA-QCS4-170921/1085
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	08-Sep-21	10	Possible buffer overflow due to 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 Networking **CVE ID : CVE-2021-1972**	https://www.qualcomm.com/company/product-security/bulletins/august-2021-bulletin	H-QUA-QCS4-170921/1086
qcs603					
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 Voice & Music, Snapdragon Wearables **CVE ID : CVE-2021-1904**	qualcomm.com/company/product-security/bulletins/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.com/company/product-security/bulletins/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.com/company/product-security/bulletins/august-2021-bulletin	H-QUA-QCS6-170921/1089

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2021-1916		
Integer Underflow (Wrap or Wraparound)	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.com/company/product-security/bulletins/august-2021-bulletin	H-QUA-QCS6-170921/1090
Integer Underflow (Wrap or Wraparound)	08-Sep-21	10	Integer underflow can occur due to improper 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.com/company/product-security/bulletins/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.com/company/product-security/bulletins/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 Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1972**	m/company/product-security/bulletins/august-2021-bulletin	
qcs605					
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.com/company/product-security/bulletins/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.com/company/product-security/bulletins/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 **CVE ID : CVE-2021-1916**	https://www.qualcomm.com/company/product-security/bulletins/august-2021-bulletin	H-QUA-QCS6-170921/1096
Integer Underflow (Wrap or Wraparound)	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.com/company/product-security/bulletins/august-2021-bulletin	H-QUA-QCS6-170921/1097
Integer Underflow (Wrap or Wraparound)	08-Sep-21	10	Integer underflow can occur due to improper 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.com/company/product-security/bulletins/august-2021-bulletin	H-QUA-QCS6-170921/1098

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.com/company/product-security/bulletins/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 Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1972**	https://www.qualcomm.com/company/product-security/bulletins/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.com/company/product-security/bulletins/august-2021-bulletin	H-QUA-QCS6-170921/1101

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.com/company/product-security/bulletins/august-2021-bulletin	H-QUA-QCS6-170921/1102
Out-of-bounds Write	08-Sep-21	10	Possible buffer underflow due to lack of check for negative indices values when 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.com/company/product-security/bulletins/august-2021-bulletin	H-QUA-QCS6-170921/1103
Integer Underflow (Wrap or Wraparound)	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.com/company/product-security/bulletins/august-2021-bulletin	H-QUA-QCS6-170921/1104

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 Wraparound)	08-Sep-21	10	Integer underflow can occur due to improper 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.com/company/product-security/bulletins/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.com/company/product-security/bulletins/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.com/company/product-security/bulletins/august-2021-bulletin	H-QUA-QCS6-170921/1107

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 Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1972**	https://www.qualcomm.com/company/product-security/bulletins/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.com/company/product-security/bulletins/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.com/company/product-security/bulletins/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 **CVE ID : CVE-2021-1916**	https://www.qualcomm.com/company/product-security/bulletins/august-2021-bulletin	H-QUA-QCS6-170921/1111
Integer Underflow (Wrap or Wraparound)	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.com/company/product-security/bulletins/august-2021-bulletin	H-QUA-QCS6-170921/1112
Integer Underflow (Wrap or Wraparound)	08-Sep-21	10	Integer underflow can occur 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.com/company/product-security/bulletins/august-2021-bulletin	H-QUA-QCS6-170921/1113

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.com/company/product-security/bulletins/august-2021-bulletin	H-QUA-QCS6-170921/1114
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.com/company/product-security/bulletins/august-2021-bulletin	H-QUA-QCS6-170921/1115
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	08-Sep-21	10	Possible buffer overflow due to 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 Networking	https://www.qualcomm.com/company/product-security/bulletins/august-2021-bulletin	H-QUA-QCS6-170921/1116

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.com/company/product-security/bulletins/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.com/company/product-security/bulletins/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.com/company/product-security/bulletins/august-2021-bulletin	H-QUA-QCX3-170921/1119

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 Wraparound)	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.com/company/product-security/bulletins/august-2021-bulletin	H-QUA-QCX3-170921/1120
Integer Underflow (Wrap or Wraparound)	08-Sep-21	10	Integer underflow can occur due to improper 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.com/company/product-security/bulletins/august-2021-bulletin	H-QUA-QCX3-170921/1121
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	08-Sep-21	10	Possible buffer overflow due to 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.com/company/product-security/bulletins/august-2021-bulletin	H-QUA-QCX3-170921/1122

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1972**		
qet4101					
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.com/company/product-security/bulletins/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.com/company/product-security/bulletins/august-2021-bulletin	H-QUA-QFE1-170921/1124
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.com/company/product-	H-QUA-QFE1-170921/1125

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/bulletins/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.com/company/product-security/bulletins/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 Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and	https://www.qualcomm.com/company/product-security/bulletins/august-2021-bulletin	H-QUA-QFE1-170921/1127

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 Voice & Music, Snapdragon Wearables **CVE ID : CVE-2021-1904**	https://www.qualcomm.com/company/product-security/bulletins/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.com/company/product-security/bulletins/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.com/company/product-security/bulletins/august-2021-bulletin	H-QUA-QRB5-170921/1130

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 Voice & Music, Snapdragon Wearables **CVE ID : CVE-2021-1904**	https://www.qualcomm.com/company/product-security/bulletins/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.com/company/product-security/bulletins/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.com/company/product-security/bulletins/august-2021-bulletin	H-QUA-QSM8-170921/1133

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.com/company/product-security/bulletins/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.com/company/product-security/bulletins/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.com/company/product-security/bulletins/august-2021-bulletin	H-QUA-QSW8-170921/1136

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 **CVE ID : CVE-2021-1916**	https://www.qualcomm.com/company/product-security/bulletins/august-2021-bulletin	H-QUA-QSW8-170921/1137
Integer Underflow (Wrap or Wraparound)	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.com/company/product-security/bulletins/august-2021-bulletin	H-QUA-QSW8-170921/1138
Integer Underflow (Wrap or Wraparound)	08-Sep-21	10	Integer underflow can occur due to improper 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.com/company/product-security/bulletins/august-2021-bulletin	H-QUA-QSW8-170921/1139

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2021-1920		
qualcomm215					
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.com/company/product-security/bulletins/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.com/company/product-security/bulletins/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.com/company/product-security/bulletins/august-2021-bulletin	H-QUA-QUAL-170921/1142

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 Wraparound)	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.com/company/product-security/bulletins/august-2021-bulletin	H-QUA-QUAL-170921/1143
Integer Underflow (Wrap or Wraparound)	08-Sep-21	10	Integer underflow can occur due to improper 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.com/company/product-security/bulletins/august-2021-bulletin	H-QUA-QUAL-170921/1144
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.com/company/product-security/bulletins/august-2021-bulletin	H-QUA-QUAL-170921/1145

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.com/company/product-security/bulletins/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 Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1972**	https://www.qualcomm.com/company/product-security/bulletins/august-2021-bulletin	H-QUA-QUAL-170921/1147
sa415m					
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.com/company/product-security/bulletins/august-2021-bulletin	H-QUA-SA41-170921/1148

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 IoT, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2021-1914**	https://www.qualcomm.com/company/product-security/bulletins/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.com/company/product-security/bulletins/august-2021-bulletin	H-QUA-SA41-170921/1150
Integer Underflow (Wrap or Wraparound)	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.com/company/product-security/bulletins/august-	H-QUA-SA41-170921/1151

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 Wraparound)	08-Sep-21	10	Integer underflow can occur due to improper 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.com/company/product-security/bulletins/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.com/company/product-security/bulletins/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.com/company/product-security/bulletins/august-2021-bulletin	H-QUA-SA41-170921/1154

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.com/company/product-security/bulletins/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.com/company/product-security/bulletins/august-2021-bulletin	H-QUA-SA51-170921/1156
Integer Underflow (Wrap or Wraparound)	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.com/company/product-security/bulletins/august-	H-QUA-SA51-170921/1157

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 Wraparound)	08-Sep-21	10	Integer underflow can occur due to improper 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.com/company/product-security/bulletins/august-2021-bulletin	H-QUA-SA51-170921/1158
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	08-Sep-21	10	Possible buffer overflow due to 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 Networking **CVE ID : CVE-2021-1972**	https://www.qualcomm.com/company/product-security/bulletins/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.com/company/product-	H-QUA-SA61-170921/1160

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/bulletins/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.com/company/product-security/bulletins/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.com/company/product-security/bulletins/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.com/company/product-security/bulletins/august-	H-QUA-SA61-170921/1163

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wearables **CVE ID : CVE-2021-1929**	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.com/company/product-security/bulletins/august-2021-bulletin	H-QUA-SA61-170921/1164
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	08-Sep-21	10	Possible buffer overflow due to 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 Networking **CVE ID : CVE-2021-1972**	https://www.qualcomm.com/company/product-security/bulletins/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.com/company/product-security/bulletins/august-2021-bulletin	H-QUA-SA61-170921/1166

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.com/company/product-security/bulletins/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.com/company/product-security/bulletins/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.com/company/product-security/bulletins/august-2021-bulletin	H-QUA-SA61-170921/1169

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			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.com/company/product-security/bulletins/august-2021-bulletin	H-QUA-SA61-170921/1170
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	08-Sep-21	10	Possible buffer overflow due to 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 Networking **CVE ID : CVE-2021-1972**	https://www.qualcomm.com/company/product-security/bulletins/august-2021-bulletin	H-QUA-SA61-170921/1171
sa6155					
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.com/company/product-security/bulletins/august-2021-bulletin	H-QUA-SA61-170921/1172

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 Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2021-1916**	https://www.qualcomm.com/company/product-security/bulletins/august-2021-bulletin	H-QUA-SA61-170921/1173
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.com/company/product-security/bulletins/august-2021-bulletin	H-QUA-SA61-170921/1174
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.com/company/product-security/bulletins/august-2021-bulletin	H-QUA-SA61-170921/1175
Buffer Copy without	08-Sep-21	10	Possible buffer overflow due to improper validation of	https://www.qualcomm.co	H-QUA-SA61-

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 Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1972**	m/company/product-security/bulletins/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 Voice & Music, Snapdragon Wearables **CVE ID : CVE-2021-1904**	https://www.qualcomm.com/company/product-security/bulletins/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.com/company/product-security/bulletins/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.com/company/product-security/bulletins/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.com/company/product-security/bulletins/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.com/company/product-security/bulletins/august-2021-bulletin	H-QUA-SA61-170921/1181
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.com/company/product-security/bulletins/august-	H-QUA-SA61-170921/1182

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.com/company/product-security/bulletins/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.com/company/product-security/bulletins/august-2021-bulletin	H-QUA-SA81-170921/1184
Incorrect	08-Sep-21	4.6	Incorrect pointer argument	https://www.	H-QUA-SA81-

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.com/company/product-security/bulletins/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.com/company/product-security/bulletins/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.com/company/product-security/bulletins/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.com/company/product-security/bulletins/august-2021-bulletin	H-QUA-SA81-170921/1188

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 Voice & Music, Snapdragon Wearables **CVE ID : CVE-2021-1904**	https://www.qualcomm.com/company/product-security/bulletins/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.com/company/product-security/bulletins/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.com/company/product-	H-QUA-SA81-170921/1191

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/bulletins/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.com/company/product-security/bulletins/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.com/company/product-security/bulletins/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 Voice & Music, Snapdragon Wearables, Snapdragon Wired	https://www.qualcomm.com/company/product-security/bulletins/august-2021-bulletin	H-QUA-SA81-170921/1194

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Infrastructure and Networking **CVE ID : CVE-2021-1972**		
sa8155					
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.com/company/product-security/bulletins/august-2021-bulletin	H-QUA-SA81-170921/1195
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.com/company/product-security/bulletins/august-2021-bulletin	H-QUA-SA81-170921/1196
Out-of-bounds Write	08-Sep-21	10	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.com/company/product-security/bulletins/august-2021-bulletin	H-QUA-SA81-170921/1197

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 Wraparound)	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.com/company/product-security/bulletins/august-2021-bulletin	H-QUA-SA81-170921/1198
Integer Underflow (Wrap or Wraparound)	08-Sep-21	10	Integer underflow can occur due to improper 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.com/company/product-security/bulletins/august-2021-bulletin	H-QUA-SA81-170921/1199
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.com/company/product-security/bulletins/august-2021-bulletin	H-QUA-SA81-170921/1200

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.com/company/product-security/bulletins/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.com/company/product-security/bulletins/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 Mobile, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1972**	https://www.qualcomm.com/company/product-security/bulletins/august-2021-bulletin	H-QUA-SA81-170921/1203
sa8155p					

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.com/company/product-security/bulletins/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.com/company/product-security/bulletins/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.com/company/product-security/bulletins/august-2021-bulletin	H-QUA-SA81-170921/1206

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2021-1916		
Integer Underflow (Wrap or Wraparound)	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.com/company/product-security/bulletins/august-2021-bulletin	H-QUA-SA81-170921/1207
Integer Underflow (Wrap or Wraparound)	08-Sep-21	10	Integer underflow can occur due to improper 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.com/company/product-security/bulletins/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.com/company/product-security/bulletins/august-2021-bulletin	H-QUA-SA81-170921/1209
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.com/company/product-	H-QUA-SA81-170921/1210

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/bulletins/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.com/company/product-security/bulletins/august-2021-bulletin	H-QUA-SA81-170921/1211
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	08-Sep-21	10	Possible buffer overflow due to 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 Networking **CVE ID : CVE-2021-1972**	https://www.qualcomm.com/company/product-security/bulletins/august-2021-bulletin	H-QUA-SA81-170921/1212
sa8195p					
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.com/company/product-security/bull	H-QUA-SA81-170921/1213

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 Write	08-Sep-21	10	Possible buffer underflow due to lack of check for negative indices values when 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.com/company/product-security/bulletins/august-2021-bulletin	H-QUA-SA81-170921/1214
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.com/company/product-security/bulletins/august-2021-bulletin	H-QUA-SA81-170921/1215
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.com/company/product-security/bulletins/august-2021-bulletin	H-QUA-SA81-170921/1216

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.com/company/product-security/bulletins/august-2021-bulletin	H-QUA-SA81-170921/1217
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	08-Sep-21	10	Possible buffer overflow due to 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 Networking **CVE ID : CVE-2021-1972**	https://www.qualcomm.com/company/product-security/bulletins/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.com/company/product-security/bulletins/august-2021-bulletin	H-QUA-SC81-170921/1219

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.com/company/product-security/bulletins/august-2021-bulletin	H-QUA-SC81-170921/1220
Integer Underflow (Wrap or Wraparound)	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.com/company/product-security/bulletins/august-2021-bulletin	H-QUA-SC81-170921/1221
Integer Underflow (Wrap or Wraparound)	08-Sep-21	10	Integer 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.com/company/product-security/bulletins/august-2021-bulletin	H-QUA-SC81-170921/1222

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 Voice & Music, Snapdragon Wearables **CVE ID : CVE-2021-1904**	https://www.qualcomm.com/company/product-security/bulletins/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.com/company/product-security/bulletins/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.com/company/product-security/bulletins/august-	H-QUA-SD20-170921/1225

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-2021-1916**	2021-bulletin	
Integer Underflow (Wrap or Wraparound)	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.com/company/product-security/bulletins/august-2021-bulletin	H-QUA-SD20-170921/1226
Integer Underflow (Wrap or Wraparound)	08-Sep-21	10	Integer underflow can occur due to improper 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.com/company/product-security/bulletins/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.com/company/product-security/bulletins/august-2021-bulletin	H-QUA-SD20-170921/1228

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.com/company/product-security/bulletins/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 Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1972**	https://www.qualcomm.com/company/product-security/bulletins/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.com/company/product-security/bull	H-QUA-SD21-170921/1231

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.com/company/product-security/bulletins/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.com/company/product-security/bulletins/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.com/company/	H-QUA-SD21-170921/1234

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Wraparound)			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/bulletins/august-2021-bulletin	
Integer Underflow (Wrap or Wraparound)	08-Sep-21	10	Integer underflow can occur due to improper 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.com/company/product-security/bulletins/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.com/company/product-security/bulletins/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.com/company/product-	H-QUA-SD21-170921/1237

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/bulletins/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 Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1972**	https://www.qualcomm.com/company/product-security/bulletins/august-2021-bulletin	H-QUA-SD21-170921/1238
sd429					
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.com/company/product-security/bulletins/august-2021-bulletin	H-QUA-SD42-170921/1239
Loop with	08-Sep-21	5	Loop with unreachable exit	https://www.	H-QUA-SD42-

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.com/company/product-security/bulletins/august-2021-bulletin	170921/1240
Out-of-bounds Write	08-Sep-21	10	Possible buffer underflow due to lack of check for negative indices values when 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.com/company/product-security/bulletins/august-2021-bulletin	H-QUA-SD42-170921/1241
Integer Underflow (Wrap or Wraparound)	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.com/company/product-security/bulletins/august-2021-bulletin	H-QUA-SD42-170921/1242
Integer	08-Sep-21	10	Integer underflow can occur	https://www.	H-QUA-SD42-

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Underflow (Wrap or Wraparound)			due to improper 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.com/company/product-security/bulletins/august-2021-bulletin	170921/1243
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	08-Sep-21	10	Possible buffer overflow due to 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 Networking **CVE ID : CVE-2021-1972**	https://www.qualcomm.com/company/product-security/bulletins/august-2021-bulletin	H-QUA-SD42-170921/1244
sd439					
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.com/company/product-security/bulletins/august-2021-bulletin	H-QUA-SD43-170921/1245

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.com/company/product-security/bulletins/august-2021-bulletin	H-QUA-SD43-170921/1246
Out-of-bounds Write	08-Sep-21	10	Possible buffer underflow due to lack of check for negative indices values when 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.com/company/product-security/bulletins/august-2021-bulletin	H-QUA-SD43-170921/1247
Integer Underflow (Wrap or Wraparound)	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.com/company/product-security/bulletins/august-2021-bulletin	H-QUA-SD43-170921/1248

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Wearables **CVE ID : CVE-2021-1919**		
Integer Underflow (Wrap or Wraparound)	08-Sep-21	10	Integer underflow can occur due to improper 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.com/company/product-security/bulletins/august-2021-bulletin	H-QUA-SD43-170921/1249
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	08-Sep-21	10	Possible buffer overflow due to 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 Networking **CVE ID : CVE-2021-1972**	https://www.qualcomm.com/company/product-security/bulletins/august-2021-bulletin	H-QUA-SD43-170921/1250
sd450					
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.com/company/product-security/bulletins/august-2021-bulletin	H-QUA-SD45-170921/1251

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 IoT, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2021-1914**	https://www.qualcomm.com/company/product-security/bulletins/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.com/company/product-security/bulletins/august-2021-bulletin	H-QUA-SD45-170921/1253
Integer Underflow (Wrap or Wraparound)	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.com/company/product-security/bulletins/august-	H-QUA-SD45-170921/1254

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 Wraparound)	08-Sep-21	10	Integer underflow can occur due to improper 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.com/company/product-security/bulletins/august-2021-bulletin	H-QUA-SD45-170921/1255
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	08-Sep-21	10	Possible buffer overflow due to 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 Networking **CVE ID : CVE-2021-1972**	https://www.qualcomm.com/company/product-security/bulletins/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.com/company/product-	H-QUA-SD46-170921/1257

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/bulletins/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.com/company/product-security/bulletins/august-2021-bulletin	H-QUA-SD46-170921/1258
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.com/company/product-security/bulletins/august-2021-bulletin	H-QUA-SD46-170921/1259
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.com/company/product-security/bulletins/august-2021-bulletin	H-QUA-SD46-170921/1260

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 Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1972**	https://www.qualcomm.com/company/product-security/bulletins/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 Voice & Music, Snapdragon Wearables **CVE ID : CVE-2021-1904**	https://www.qualcomm.com/company/product-security/bulletins/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.com/company/product-security/bulletins/august-	H-QUA-SD48-170921/1263

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.com/company/product-security/bulletins/august-2021-bulletin	H-QUA-SD48-170921/1264
Integer Underflow (Wrap or Wraparound)	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.com/company/product-security/bulletins/august-2021-bulletin	H-QUA-SD48-170921/1265
Integer Underflow (Wrap or Wraparound)	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.com/company/product-security/bulletins/august-	H-QUA-SD48-170921/1266

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.com/company/product-security/bulletins/august-2021-bulletin	H-QUA-SD48-170921/1267
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.com/company/product-security/bulletins/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.com/company/product-security/bulletins/august-2021-bulletin	H-QUA-SD48-170921/1269
Buffer Copy without	08-Sep-21	10	Possible buffer overflow due to improper validation of	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 Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1972**	m/company/product-security/bulletins/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.com/company/product-security/bulletins/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.com/company/product-security/bulletins/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 **CVE ID : CVE-2021-1916**	https://www.qualcomm.com/company/product-security/bulletins/august-2021-bulletin	H-QUA-SD63-170921/1273
Integer Underflow (Wrap or Wraparound)	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.com/company/product-security/bulletins/august-2021-bulletin	H-QUA-SD63-170921/1274
Integer Underflow (Wrap or Wraparound)	08-Sep-21	10	Integer underflow can occur due to improper 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.com/company/product-security/bulletins/august-2021-bulletin	H-QUA-SD63-170921/1275

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 Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1972**	https://www.qualcomm.com/company/product-security/bulletins/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 Voice & Music, Snapdragon Wearables **CVE ID : CVE-2021-1904**	https://www.qualcomm.com/company/product-security/bulletins/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.com/company/product-security/bulletins/august-2021-bulletin	H-QUA-SD66-170921/1278

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**		
sd662					
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.com/company/product-security/bulletins/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.com/company/product-security/bulletins/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.com/company/product-security/bulletins/august-	H-QUA-SD66-170921/1281

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wearables **CVE ID : CVE-2021-1929**	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.com/company/product-security/bulletins/august-2021-bulletin	H-QUA-SD66-170921/1282
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	08-Sep-21	10	Possible buffer overflow due to 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 Networking **CVE ID : CVE-2021-1972**	https://www.qualcomm.com/company/product-security/bulletins/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.com/company/product-security/bulletins/august-2021-bulletin	H-QUA-SD66-170921/1284

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.com/company/product-security/bulletins/august-2021-bulletin	H-QUA-SD66-170921/1285
Out-of-bounds Write	08-Sep-21	10	Possible buffer underflow due to lack of check for negative indices values when 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.com/company/product-security/bulletins/august-2021-bulletin	H-QUA-SD66-170921/1286
Integer Underflow (Wrap or Wraparound)	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.com/company/product-security/bull	H-QUA-SD66-170921/1287

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-2021-1919**	etins/august-2021-bulletin	
Integer Underflow (Wrap or Wraparound)	08-Sep-21	10	Integer underflow can occur due to improper 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.com/company/product-security/bulletins/august-2021-bulletin	H-QUA-SD66-170921/1288
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.com/company/product-security/bulletins/august-2021-bulletin	H-QUA-SD66-170921/1289
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.com/company/product-security/bulletins/august-2021-bulletin	H-QUA-SD66-170921/1290

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.com/company/product-security/bulletins/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 Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1972**	https://www.qualcomm.com/company/product-security/bulletins/august-2021-bulletin	H-QUA-SD66-170921/1292
sd670					
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.com/company/product-security/bulletins/august-2021-bulletin	H-QUA-SD67-170921/1293

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.com/company/product-security/bulletins/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.com/company/product-security/bulletins/august-2021-bulletin	H-QUA-SD67-170921/1295
Integer Underflow (Wrap or Wraparound)	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.com/company/product-security/bulletins/august-2021-bulletin	H-QUA-SD67-170921/1296

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Voice & Music, Snapdragon Wearables **CVE ID : CVE-2021-1919**		
Integer Underflow (Wrap or Wraparound)	08-Sep-21	10	Integer underflow can occur due to improper 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.com/company/product-security/bulletins/august-2021-bulletin	H-QUA-SD67-170921/1297
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.com/company/product-security/bulletins/august-2021-bulletin	H-QUA-SD67-170921/1298
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.com/company/product-security/bulletins/august-2021-bulletin	H-QUA-SD67-170921/1299
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.com/company/product-	H-QUA-SD67-170921/1300

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/bulletins/august-2021-bulletin	
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.com/company/product-security/bulletins/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.com/company/product-security/bulletins/august-2021-bulletin	H-QUA-SD67-170921/1302

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.com/company/product-security/bulletins/august-2021-bulletin	H-QUA-SD67-170921/1303
Integer Underflow (Wrap or Wraparound)	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.com/company/product-security/bulletins/august-2021-bulletin	H-QUA-SD67-170921/1304
Integer Underflow (Wrap or Wraparound)	08-Sep-21	10	Integer underflow can occur due to improper 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.com/company/product-security/bulletins/august-2021-bulletin	H-QUA-SD67-170921/1305

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.com/company/product-security/bulletins/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.com/company/product-security/bulletins/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.com/company/product-security/bulletins/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.com/company/product-security/bulletins/august-2021-bulletin	H-QUA-SD67-170921/1309

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					
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.com/company/product-security/bulletins/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.com/company/product-security/bulletins/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.com/company/	H-QUA-SD67-170921/1312

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/bulletins/august-2021-bulletin	
Integer Underflow (Wrap or Wraparound)	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.com/company/product-security/bulletins/august-2021-bulletin	H-QUA-SD67-170921/1313
Integer Underflow (Wrap or Wraparound)	08-Sep-21	10	Integer underflow can occur due to improper 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.com/company/product-security/bulletins/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.com/company/product-	H-QUA-SD67-170921/1315

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/bulletins/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.com/company/product-security/bulletins/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.com/company/product-security/bulletins/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 Voice & Music, Snapdragon Wearables, Snapdragon Wired	https://www.qualcomm.com/company/product-security/bulletins/august-2021-bulletin	H-QUA-SD67-170921/1318

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Infrastructure and Networking **CVE ID : CVE-2021-1972**		
sd690_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.com/company/product-security/bulletins/august-2021-bulletin	H-QUA-SD69-170921/1319
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.com/company/product-security/bulletins/august-2021-bulletin	H-QUA-SD69-170921/1320
Out-of-bounds Write	08-Sep-21	10	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.com/company/product-security/bulletins/august-2021-bulletin	H-QUA-SD69-170921/1321

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 Wraparound)	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.com/company/product-security/bulletins/august-2021-bulletin	H-QUA-SD69-170921/1322
Integer Underflow (Wrap or Wraparound)	08-Sep-21	10	Integer underflow can occur due to improper 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.com/company/product-security/bulletins/august-2021-bulletin	H-QUA-SD69-170921/1323
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.com/company/product-security/bulletins/august-2021-bulletin	H-QUA-SD69-170921/1324

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.com/company/product-security/bulletins/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 Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1972**	https://www.qualcomm.com/company/product-security/bulletins/august-2021-bulletin	H-QUA-SD69-170921/1326
sd710					
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.com/company/product-security/bulletins/august-2021-bulletin	H-QUA-SD71-170921/1327

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2021-1904**		
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.com/company/product-security/bulletins/august-2021-bulletin	H-QUA-SD71-170921/1328
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	08-Sep-21	10	Possible buffer overflow due to 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 Networking **CVE ID : CVE-2021-1972**	https://www.qualcomm.com/company/product-security/bulletins/august-2021-bulletin	H-QUA-SD71-170921/1329
sd712					
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.com/company/product-security/bulletins/august-2021-bulletin	H-QUA-SD71-170921/1330

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.com/company/product-security/bulletins/august-2021-bulletin	H-QUA-SD71-170921/1331
Integer Underflow (Wrap or Wraparound)	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.com/company/product-security/bulletins/august-2021-bulletin	H-QUA-SD71-170921/1332
Integer Underflow (Wrap or Wraparound)	08-Sep-21	10	Integer underflow can occur 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.com/company/product-security/bulletins/august-2021-bulletin	H-QUA-SD71-170921/1333

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 Voice & Music, Snapdragon Wearables **CVE ID : CVE-2021-1904**	https://www.qualcomm.com/company/product-security/bulletins/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.com/company/product-security/bulletins/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.com/company/product-security/bulletins/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 Wraparound)	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.com/company/product-security/bulletins/august-2021-bulletin	H-QUA-SD72-170921/1337
Integer Underflow (Wrap or Wraparound)	08-Sep-21	10	Integer underflow can occur due to improper 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.com/company/product-security/bulletins/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.com/company/product-security/bulletins/august-2021-bulletin	H-QUA-SD72-170921/1339

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.com/company/product-security/bulletins/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.com/company/product-security/bulletins/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 Mobile, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1972**	https://www.qualcomm.com/company/product-security/bulletins/august-2021-bulletin	H-QUA-SD72-170921/1342
sd730					

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.com/company/product-security/bulletins/august-2021-bulletin	H-QUA-SD73-170921/1343
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.com/company/product-security/bulletins/august-2021-bulletin	H-QUA-SD73-170921/1344
Out-of-bounds Write	08-Sep-21	10	Possible buffer underflow due to lack of check for negative indices values when 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.com/company/product-security/bulletins/august-2021-bulletin	H-QUA-SD73-170921/1345

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2021-1916		
Integer Underflow (Wrap or Wraparound)	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.com/company/product-security/bulletins/august-2021-bulletin	H-QUA-SD73-170921/1346
Integer Underflow (Wrap or Wraparound)	08-Sep-21	10	Integer underflow can occur due to improper 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.com/company/product-security/bulletins/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.com/company/product-security/bulletins/august-2021-bulletin	H-QUA-SD73-170921/1348
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.com/company/product-	H-QUA-SD73-170921/1349

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/bulletins/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.com/company/product-security/bulletins/august-2021-bulletin	H-QUA-SD73-170921/1350
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	08-Sep-21	10	Possible buffer overflow due to 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 Networking **CVE ID : CVE-2021-1972**	https://www.qualcomm.com/company/product-security/bulletins/august-2021-bulletin	H-QUA-SD73-170921/1351
sd750g					
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.com/company/product-security/bull	H-QUA-SD75-170921/1352

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.com/company/product-security/bulletins/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.com/company/product-security/bulletins/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.com/company/	H-QUA-SD75-170921/1355

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Wraparound)			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/bulletins/august-2021-bulletin	
Integer Underflow (Wrap or Wraparound)	08-Sep-21	10	Integer underflow can occur due to improper 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.com/company/product-security/bulletins/august-2021-bulletin	H-QUA-SD75-170921/1356
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.com/company/product-security/bulletins/august-2021-bulletin	H-QUA-SD75-170921/1357
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.com/company/product-security/bulletins/august-2021-bulletin	H-QUA-SD75-170921/1358

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 Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1972**	https://www.qualcomm.com/company/product-security/bulletins/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 Voice & Music, Snapdragon Wearables **CVE ID : CVE-2021-1904**	https://www.qualcomm.com/company/product-security/bulletins/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.com/company/product-security/bulletins/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.com/company/product-security/bulletins/august-2021-bulletin	H-QUA-SD76-170921/1362
Integer Underflow (Wrap or Wraparound)	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.com/company/product-security/bulletins/august-2021-bulletin	H-QUA-SD76-170921/1363
Integer Underflow (Wrap or Wraparound)	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.com/company/product-security/bulletins/august-	H-QUA-SD76-170921/1364

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.com/company/product-security/bulletins/august-2021-bulletin	H-QUA-SD76-170921/1365
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.com/company/product-security/bulletins/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.com/company/product-security/bulletins/august-2021-bulletin	H-QUA-SD76-170921/1367
Buffer Copy without	08-Sep-21	10	Possible buffer overflow due to improper validation of	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 Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1972**	m/company/product-security/bulletins/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.com/company/product-security/bulletins/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.com/company/product-security/bulletins/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 **CVE ID : CVE-2021-1916**	https://www.qualcomm.com/company/product-security/bulletins/august-2021-bulletin	H-QUA-SD76-170921/1371
Integer Underflow (Wrap or Wraparound)	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.com/company/product-security/bulletins/august-2021-bulletin	H-QUA-SD76-170921/1372
Integer Underflow (Wrap or Wraparound)	08-Sep-21	10	Integer underflow can occur due to improper 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.com/company/product-security/bulletins/august-2021-bulletin	H-QUA-SD76-170921/1373

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.com/company/product-security/bulletins/august-2021-bulletin	H-QUA-SD76-170921/1374
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.com/company/product-security/bulletins/august-2021-bulletin	H-QUA-SD76-170921/1375
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.com/company/product-security/bulletins/august-2021-bulletin	H-QUA-SD76-170921/1376
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	08-Sep-21	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.com/company/product-security/bulletins/august-2021-bulletin	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 Voice & Music, Snapdragon Wearables **CVE ID : CVE-2021-1904**	https://www.qualcomm.com/company/product-security/bulletins/august-2021-bulletin	H-QUA-SD76-170921/1378
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.com/company/product-security/bulletins/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/bulletins/august-2021-bulletin	
Integer Underflow (Wrap or Wraparound)	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.com/company/product-security/bulletins/august-2021-bulletin	H-QUA-SD76-170921/1381
Integer Underflow (Wrap or Wraparound)	08-Sep-21	10	Integer underflow can occur due to improper 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.com/company/product-security/bulletins/august-2021-bulletin	H-QUA-SD76-170921/1382
Incorrect Type Conversion	08-Sep-21	4.6	Incorrect pointer argument passed to trusted application TA could result in un-	https://www.qualcomm.com/company/	H-QUA-SD76-170921/1383

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/bulletins/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.com/company/product-security/bulletins/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.com/company/product-security/bulletins/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.com/company/product-security/bulletins/august-2021-bulletin	H-QUA-SD76-170921/1386

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 Voice & Music, Snapdragon Wearables **CVE ID : CVE-2021-1904**	https://www.qualcomm.com/company/product-security/bulletins/august-2021-bulletin	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.com/company/product-security/bulletins/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.com/company/product-security/bulletins/august-	H-QUA-SD77-170921/1389

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-2021-1916**	2021-bulletin	
Integer Underflow (Wrap or Wraparound)	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.com/company/product-security/bulletins/august-2021-bulletin	H-QUA-SD77-170921/1390
Integer Underflow (Wrap or Wraparound)	08-Sep-21	10	Integer underflow can occur due to improper 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.com/company/product-security/bulletins/august-2021-bulletin	H-QUA-SD77-170921/1391
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.com/company/product-security/bulletins/august-2021-bulletin	H-QUA-SD77-170921/1392

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.com/company/product-security/bulletins/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.com/company/product-security/bulletins/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 Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1972**	https://www.qualcomm.com/company/product-security/bulletins/august-2021-bulletin	H-QUA-SD77-170921/1395

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
sd780g					
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.com/company/product-security/bulletins/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.com/company/product-security/bulletins/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.com/company/product-security/bulletins/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-

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.com/company/product-security/bulletins/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.com/company/product-security/bulletins/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 Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1972**	https://www.qualcomm.com/company/product-security/bulletins/august-2021-bulletin	H-QUA-SD78-170921/1401
sd7c					
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

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/bulletins/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 IoT, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2021-1914**	https://www.qualcomm.com/company/product-security/bulletins/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.com/company/product-security/bulletins/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.com/company/	H-QUA-SD82-170921/1405

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Wraparound)			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/bulletins/august-2021-bulletin	
Integer Underflow (Wrap or Wraparound)	08-Sep-21	10	Integer underflow can occur due to improper 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.com/company/product-security/bulletins/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.com/company/product-security/bulletins/august-2021-bulletin	H-QUA-SD82-170921/1407
Out-of-bounds Write	08-Sep-21	10	Possible buffer underflow due to lack of check for negative indices values when	https://www.qualcomm.com/company/	H-QUA-SD82-170921/1408

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/bulletins/august-2021-bulletin	
Integer Underflow (Wrap or Wraparound)	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.com/company/product-security/bulletins/august-2021-bulletin	H-QUA-SD82-170921/1409
Integer Underflow (Wrap or Wraparound)	08-Sep-21	10	Integer underflow can occur due to improper 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.com/company/product-security/bulletins/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.com/company/	H-QUA-SD83-170921/1411

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/bulletins/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.com/company/product-security/bulletins/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.com/company/product-security/bulletins/august-2021-bulletin	H-QUA-SD83-170921/1413
Integer	08-Sep-21	10	Integer underflow can occur	https://www.	H-QUA-SD83-

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Underflow (Wrap or Wraparound)			when 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.com/company/product-security/bulletins/august-2021-bulletin	170921/1414
Integer Underflow (Wrap or Wraparound)	08-Sep-21	10	Integer underflow can occur due to improper 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.com/company/product-security/bulletins/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 Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1972**	https://www.qualcomm.com/company/product-security/bulletins/august-2021-bulletin	H-QUA-SD83-170921/1416

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
sd845					
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.com/company/product-security/bulletins/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.com/company/product-security/bulletins/august-2021-bulletin	H-QUA-SD84-170921/1418
Out-of-bounds Write	08-Sep-21	10	Possible buffer underflow due to lack of check for negative indices values 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.com/company/product-security/bulletins/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 Wraparound)	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.com/company/product-security/bulletins/august-2021-bulletin	H-QUA-SD84-170921/1420
Integer Underflow (Wrap or Wraparound)	08-Sep-21	10	Integer underflow can occur due to improper 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.com/company/product-security/bulletins/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 Voice & Music, Snapdragon Wearables, Snapdragon Wired	https://www.qualcomm.com/company/product-security/bulletins/august-2021-bulletin	H-QUA-SD84-170921/1422

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Infrastructure and Networking **CVE ID : CVE-2021-1972**		
sd850					
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.com/company/product-security/bulletins/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.com/company/product-security/bulletins/august-2021-bulletin	H-QUA-SD85-170921/1424
Integer Underflow (Wrap or Wraparound)	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.com/company/product-security/bulletins/august-2021-bulletin	H-QUA-SD85-170921/1425

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 Wraparound)	08-Sep-21	10	Integer underflow can occur due to improper 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.com/company/product-security/bulletins/august-2021-bulletin	H-QUA-SD85-170921/1426
sd855					
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.com/company/product-security/bulletins/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.com/company/product-security/bulletins/august-2021-bulletin	H-QUA-SD85-170921/1428

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.com/company/product-security/bulletins/august-2021-bulletin	H-QUA-SD85-170921/1429
Integer Underflow (Wrap or Wraparound)	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.com/company/product-security/bulletins/august-2021-bulletin	H-QUA-SD85-170921/1430
Integer Underflow (Wrap or Wraparound)	08-Sep-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.com/company/product-security/bulletins/august-2021-bulletin	H-QUA-SD85-170921/1431

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.com/company/product-security/bulletins/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.com/company/product-security/bulletins/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.com/company/product-security/bulletins/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.com/company/	H-QUA-SD85-170921/1435

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/bulletins/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.com/company/product-security/bulletins/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.com/company/product-security/bulletins/august-2021-bulletin	H-QUA-SD86-170921/1437

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 **CVE ID : CVE-2021-1916**	https://www.qualcomm.com/company/product-security/bulletins/august-2021-bulletin	H-QUA-SD86-170921/1438
Integer Underflow (Wrap or Wraparound)	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.com/company/product-security/bulletins/august-2021-bulletin	H-QUA-SD86-170921/1439
Integer Underflow (Wrap or Wraparound)	08-Sep-21	10	Integer underflow can occur due to improper 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.com/company/product-security/bulletins/august-2021-bulletin	H-QUA-SD86-170921/1440

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.com/company/product-security/bulletins/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.com/company/product-security/bulletins/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.com/company/product-security/bulletins/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.com/company/product-security/bulletins/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 Voice & Music, Snapdragon Wearables **CVE ID : CVE-2021-1904**	https://www.qualcomm.com/company/product-security/bulletins/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.com/company/product-security/bulletins/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/bulletins/august-2021-bulletin	
Integer Underflow (Wrap or Wraparound)	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.com/company/product-security/bulletins/august-2021-bulletin	H-QUA-SD87-170921/1448
Integer Underflow (Wrap or Wraparound)	08-Sep-21	10	Integer underflow can occur due to improper 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.com/company/product-security/bulletins/august-2021-bulletin	H-QUA-SD87-170921/1449
Incorrect Type Conversion	08-Sep-21	4.6	Incorrect pointer argument passed to trusted application TA could result in un-	https://www.qualcomm.com/company/	H-QUA-SD87-170921/1450

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/bulletins/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.com/company/product-security/bulletins/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.com/company/product-security/bulletins/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.com/company/product-security/bulletins/august-2021-bulletin	H-QUA-SD87-170921/1453

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 Voice & Music, Snapdragon Wearables **CVE ID : CVE-2021-1904**	https://www.qualcomm.com/company/product-security/bulletins/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 Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1972**	https://www.qualcomm.com/company/product-security/bulletins/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.com/company/	H-QUA-SD88-170921/1456

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/bulletins/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.com/company/product-security/bulletins/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.com/company/product-security/bulletins/august-2021-bulletin	H-QUA-SD88-170921/1458
Integer	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 Wraparound)			when 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.com/company/product-security/bulletins/august-2021-bulletin	170921/1459
Integer Underflow (Wrap or Wraparound)	08-Sep-21	10	Integer underflow can occur due to improper 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.com/company/product-security/bulletins/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.com/company/product-security/bulletins/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.com/company/product-security/bulletins/august-	H-QUA-SD88-170921/1462

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wearables **CVE ID : CVE-2021-1929**	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.com/company/product-security/bulletins/august-2021-bulletin	H-QUA-SD88-170921/1463
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	08-Sep-21	10	Possible buffer overflow due to 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 Networking **CVE ID : CVE-2021-1972**	https://www.qualcomm.com/company/product-security/bulletins/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.com/company/product-security/bulletins/august-2021-bulletin	H-QUA-SDA4-170921/1465

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.com/company/product-security/bulletins/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.com/company/product-security/bulletins/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.com/company/product-security/bull	H-QUA-SDA4-170921/1468

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.com/company/product-security/bulletins/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 Voice & Music, Snapdragon Wearables **CVE ID : CVE-2021-1904**	https://www.qualcomm.com/company/product-security/bulletins/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.com/company/product-	H-QUA-SDM4-170921/1471

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/bulletins/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.com/company/product-security/bulletins/august-2021-bulletin	H-QUA-SDM4-170921/1472
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	08-Sep-21	10	Possible buffer overflow due to 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 Networking **CVE ID : CVE-2021-1972**	https://www.qualcomm.com/company/product-security/bulletins/august-2021-bulletin	H-QUA-SDM4-170921/1473
sdm630					

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.com/company/product-security/bulletins/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.com/company/product-security/bulletins/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.com/company/product-security/bulletins/august-2021-bulletin	H-QUA-SDM6-170921/1476

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2021-1916		
Integer Underflow (Wrap or Wraparound)	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.com/company/product-security/bulletins/august-2021-bulletin	H-QUA-SDM6-170921/1477
Integer Underflow (Wrap or Wraparound)	08-Sep-21	10	Integer underflow can occur due to improper 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.com/company/product-security/bulletins/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 Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and	https://www.qualcomm.com/company/product-security/bulletins/august-2021-bulletin	H-QUA-SDM6-170921/1479

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 **CVE ID : CVE-2021-1904**	https://www.qualcomm.com/company/product-security/bulletins/august-2021-bulletin	H-QUA-SDM8-170921/1480
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.com/company/product-security/bulletins/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.com/company/product-security/bulletins/august-2021-bulletin	H-QUA-SDM8-170921/1482

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 Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1972**	https://www.qualcomm.com/company/product-security/bulletins/august-2021-bulletin	H-QUA-SDM8-170921/1483
sdw2500					
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.com/company/product-security/bulletins/august-2021-bulletin	H-QUA-SDW2-170921/1484
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.com/company/product-security/bulletins/august-2021-bulletin	H-QUA-SDW2-170921/1485

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.com/company/product-security/bulletins/august-2021-bulletin	H-QUA-SDW2-170921/1486
Integer Underflow (Wrap or Wraparound)	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.com/company/product-security/bulletins/august-2021-bulletin	H-QUA-SDW2-170921/1487
Integer Underflow (Wrap or Wraparound)	08-Sep-21	10	Integer underflow can occur 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.com/company/product-security/bulletins/august-2021-bulletin	H-QUA-SDW2-170921/1488

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 Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1972**	https://www.qualcomm.com/company/product-security/bulletins/august-2021-bulletin	H-QUA-SDW2-170921/1489
sdx12					
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.com/company/product-security/bulletins/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.com/company/product-security/bull	H-QUA-SDX1-170921/1491

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.com/company/product-security/bulletins/august-2021-bulletin	H-QUA-SDX1-170921/1492
Integer Underflow (Wrap or Wraparound)	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.com/company/product-security/bulletins/august-2021-bulletin	H-QUA-SDX1-170921/1493
Integer Underflow (Wrap or Wraparound)	08-Sep-21	10	Integer underflow can occur due to improper handling of incoming RTCP packets in Snapdragon Auto, Snapdragon Compute,	https://www.qualcomm.com/company/product-security/bull	H-QUA-SDX1-170921/1494

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-2021-1920**	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 Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1972**	https://www.qualcomm.com/company/product-security/bulletins/august-2021-bulletin	H-QUA-SDX1-170921/1495
sdx20					
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.com/company/product-security/bulletins/august-2021-bulletin	H-QUA-SDX2-170921/1496
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.com/company/product-security/bulletins/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.com/company/product-security/bulletins/august-2021-bulletin	H-QUA-SDX2-170921/1498
Integer Underflow (Wrap or Wraparound)	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.com/company/product-security/bulletins/august-2021-bulletin	H-QUA-SDX2-170921/1499
Integer	08-Sep-21	10	Integer underflow can occur	https://www.	H-QUA-SDX2-

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Underflow (Wrap or Wraparound)			due to improper 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.com/company/product-security/bulletins/august-2021-bulletin	170921/1500
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	08-Sep-21	10	Possible buffer overflow due to 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 Networking **CVE ID : CVE-2021-1972**	https://www.qualcomm.com/company/product-security/bulletins/august-2021-bulletin	H-QUA-SDX2-170921/1501
sdx20m					
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.com/company/product-security/bulletins/august-2021-bulletin	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 Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1972**	https://www.qualcomm.com/company/product-security/bulletins/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 Voice & Music, Snapdragon Wearables **CVE ID : CVE-2021-1904**	https://www.qualcomm.com/company/product-security/bulletins/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.com/company/product-security/bulletins/august-	H-QUA-SDX2-170921/1505

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.com/company/product-security/bulletins/august-2021-bulletin	H-QUA-SDX2-170921/1506
Integer Underflow (Wrap or Wraparound)	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.com/company/product-security/bulletins/august-2021-bulletin	H-QUA-SDX2-170921/1507
Integer Underflow (Wrap or Wraparound)	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.com/company/product-security/bulletins/august-	H-QUA-SDX2-170921/1508

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.com/company/product-security/bulletins/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.com/company/product-security/bulletins/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 Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and	https://www.qualcomm.com/company/product-security/bulletins/august-2021-bulletin	H-QUA-SDX2-170921/1511

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 Voice & Music, Snapdragon Wearables **CVE ID : CVE-2021-1904**	https://www.qualcomm.com/company/product-security/bulletins/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.com/company/product-security/bulletins/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.com/company/product-security/bulletins/august-2021-bulletin	H-QUA-SDX5-170921/1514

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 Wraparound)	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.com/company/product-security/bulletins/august-2021-bulletin	H-QUA-SDX5-170921/1515
Integer Underflow (Wrap or Wraparound)	08-Sep-21	10	Integer underflow can occur due to improper 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.com/company/product-security/bulletins/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.com/company/product-security/bulletins/august-2021-bulletin	H-QUA-SDX5-170921/1517

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.com/company/product-security/bulletins/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.com/company/product-security/bulletins/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 Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1972**	https://www.qualcomm.com/company/product-security/bulletins/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-

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 Voice & Music, Snapdragon Wearables **CVE ID : CVE-2021-1904**	qualcomm.com/company/product-security/bulletins/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.com/company/product-security/bulletins/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.com/company/product-security/bulletins/august-2021-bulletin	H-QUA-SDX5-170921/1523

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2021-1916		
Integer Underflow (Wrap or Wraparound)	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.com/company/product-security/bulletins/august-2021-bulletin	H-QUA-SDX5-170921/1524
Integer Underflow (Wrap or Wraparound)	08-Sep-21	10	Integer underflow can occur due to improper 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.com/company/product-security/bulletins/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.com/company/product-security/bulletins/august-2021-bulletin	H-QUA-SDX5-170921/1526
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.com/company/product-	H-QUA-SDX5-170921/1527

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/bulletins/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.com/company/product-security/bulletins/august-2021-bulletin	H-QUA-SDX5-170921/1528
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	08-Sep-21	10	Possible buffer overflow due to 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 Networking **CVE ID : CVE-2021-1972**	https://www.qualcomm.com/company/product-security/bulletins/august-2021-bulletin	H-QUA-SDX5-170921/1529
sdx55m					
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.com/company/product-security/bull	H-QUA-SDX5-170921/1530

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.com/company/product-security/bulletins/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.com/company/product-security/bulletins/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.com/company/	H-QUA-SDX5-170921/1533

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Wraparound)			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/bulletins/august-2021-bulletin	
Integer Underflow (Wrap or Wraparound)	08-Sep-21	10	Integer underflow can occur due to improper 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.com/company/product-security/bulletins/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.com/company/product-security/bulletins/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.com/company/product-security/bulletins/august-2021-bulletin	H-QUA-SDX5-170921/1536

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.com/company/product-security/bulletins/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 Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1972**	https://www.qualcomm.com/company/product-security/bulletins/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.com/company/product-security/bulletins/august-2021-bulletin	H-QUA-SDXR-170921/1539

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 **CVE ID : CVE-2021-1914**	https://www.qualcomm.com/company/product-security/bulletins/august-2021-bulletin	H-QUA-SDXR-170921/1540
Out-of-bounds Write	08-Sep-21	10	Possible buffer underflow due to lack of check for negative indices values when 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.com/company/product-security/bulletins/august-2021-bulletin	H-QUA-SDXR-170921/1541
Integer Underflow (Wrap or Wraparound)	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.com/company/product-security/bulletins/august-2021-bulletin	H-QUA-SDXR-170921/1542

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 Wraparound)	08-Sep-21	10	Integer underflow can occur due to improper 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.com/company/product-security/bulletins/august-2021-bulletin	H-QUA-SDXR-170921/1543
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	08-Sep-21	10	Possible buffer overflow due to 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 Networking **CVE ID : CVE-2021-1972**	https://www.qualcomm.com/company/product-security/bulletins/august-2021-bulletin	H-QUA-SDXR-170921/1544
sdxr2_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	https://www.qualcomm.com/company/product-security/bull	H-QUA-SDXR-170921/1545

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.com/company/product-security/bulletins/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.com/company/product-security/bulletins/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.com/company/	H-QUA-SDXR-170921/1548

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Wraparound)			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/bulletins/august-2021-bulletin	
Integer Underflow (Wrap or Wraparound)	08-Sep-21	10	Integer underflow can occur due to improper 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.com/company/product-security/bulletins/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.com/company/product-security/bulletins/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.com/company/product-security/bulletins/august-2021-bulletin	H-QUA-SDXR-170921/1551

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.com/company/product-security/bulletins/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 Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1972**	https://www.qualcomm.com/company/product-security/bulletins/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.com/company/product-security/bulletins/august-2021-bulletin	H-QUA-SD_4-170921/1554

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 **CVE ID : CVE-2021-1914**	https://www.qualcomm.com/company/product-security/bulletins/august-2021-bulletin	H-QUA-SD_4-170921/1555
Out-of-bounds Write	08-Sep-21	10	Possible buffer underflow due to lack of check for negative indices values when 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.com/company/product-security/bulletins/august-2021-bulletin	H-QUA-SD_4-170921/1556
Integer Underflow (Wrap or Wraparound)	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.com/company/product-security/bulletins/august-2021-bulletin	H-QUA-SD_4-170921/1557

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 Wraparound)	08-Sep-21	10	Integer underflow can occur due to improper 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.com/company/product-security/bulletins/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 Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1972**	https://www.qualcomm.com/company/product-security/bulletins/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.com/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.com/company/product-security/bulletins/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.com/company/product-security/bulletins/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.com/company/	H-QUA-SD_6-170921/1563

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Wraparound)			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/bulletins/august-2021-bulletin	
Integer Underflow (Wrap or Wraparound)	08-Sep-21	10	Integer underflow can occur due to improper 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.com/company/product-security/bulletins/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 Mobile, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1972**	https://www.qualcomm.com/company/product-security/bulletins/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-

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 Voice & Music, Snapdragon Wearables **CVE ID : CVE-2021-1904**	qualcomm.com/company/product-security/bulletins/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.com/company/product-security/bulletins/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.com/company/product-security/bulletins/august-2021-bulletin	H-QUA-SD_6-170921/1568

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2021-1916		
Integer Underflow (Wrap or Wraparound)	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.com/company/product-security/bulletins/august-2021-bulletin	H-QUA-SD_6-170921/1569
Integer Underflow (Wrap or Wraparound)	08-Sep-21	10	Integer underflow can occur due to improper 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.com/company/product-security/bulletins/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.com/company/product-security/bulletins/august-2021-bulletin	H-QUA-SD_6-170921/1571
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.com/company/product-	H-QUA-SD_6-170921/1572

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/bulletins/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.com/company/product-security/bulletins/august-2021-bulletin	H-QUA-SD_6-170921/1573
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	08-Sep-21	10	Possible buffer overflow due to 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 Networking **CVE ID : CVE-2021-1972**	https://www.qualcomm.com/company/product-security/bulletins/august-2021-bulletin	H-QUA-SD_6-170921/1574
sd_8c					
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.com/company/product-security/bull	H-QUA-SD_8-170921/1575

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.com/company/product-security/bulletins/august-2021-bulletin	H-QUA-SD_8-170921/1576
Out-of-bounds Write	08-Sep-21	10	Possible buffer underflow due to lack of check for negative indices values when 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.com/company/product-security/bulletins/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.com/company/	H-QUA-SD_8-170921/1578

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Wraparound)			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/bulletins/august-2021-bulletin	
Integer Underflow (Wrap or Wraparound)	08-Sep-21	10	Integer underflow can occur due to improper 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.com/company/product-security/bulletins/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.com/company/product-security/bulletins/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.com/company/product-security/bulletins/august-2021-bulletin	H-QUA-SD_8-170921/1581

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 Voice & Music, Snapdragon Wearables **CVE ID : CVE-2021-1904**	https://www.qualcomm.com/company/product-security/bulletins/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.com/company/product-security/bulletins/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.com/company/	H-QUA-SD_8-170921/1584

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/bulletins/august-2021-bulletin	
Integer Underflow (Wrap or Wraparound)	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.com/company/product-security/bulletins/august-2021-bulletin	H-QUA-SD_8-170921/1585
Integer Underflow (Wrap or Wraparound)	08-Sep-21	10	Integer underflow can occur due to improper 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.com/company/product-security/bulletins/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.com/company/product-	H-QUA-SD_8-170921/1587

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/bulletins/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 Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1972**	https://www.qualcomm.com/company/product-security/bulletins/august-2021-bulletin	H-QUA-SD_8-170921/1588
sm4125					
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.com/company/product-security/bulletins/august-2021-bulletin	H-QUA-SM41-170921/1589
Incorrect Type Conversion	08-Sep-21	4.6	Incorrect pointer argument passed to trusted application TA could result in un-	https://www.qualcomm.com/company/	H-QUA-SM41-170921/1590

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/bulletins/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.com/company/product-security/bulletins/august-2021-bulletin	H-QUA-SM41-170921/1591
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	08-Sep-21	10	Possible buffer overflow due to 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 Networking **CVE ID : CVE-2021-1972**	https://www.qualcomm.com/company/product-security/bulletins/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.com/company/product-security/bulletins/august-	H-QUA-SM62-170921/1593

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	
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.com/company/product-security/bulletins/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.com/company/product-security/bulletins/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.com/company/product-	H-QUA-SM62-170921/1596

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/bulletins/august-2021-bulletin	
Integer Underflow (Wrap or Wraparound)	08-Sep-21	10	Integer underflow can occur due to improper 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.com/company/product-security/bulletins/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.com/company/product-security/bulletins/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.com/company/product-security/bulletins/august-2021-bulletin	H-QUA-SM62-170921/1599

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			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.com/company/product-security/bulletins/august-2021-bulletin	H-QUA-SM62-170921/1600
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	08-Sep-21	10	Possible buffer overflow due to 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 Networking **CVE ID : CVE-2021-1972**	https://www.qualcomm.com/company/product-security/bulletins/august-2021-bulletin	H-QUA-SM62-170921/1601
sm6250p					
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.com/company/product-security/bulletins/august-2021-bulletin	H-QUA-SM62-170921/1602

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.com/company/product-security/bulletins/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.com/company/product-security/bulletins/august-2021-bulletin	H-QUA-SM62-170921/1604
Integer Underflow (Wrap or Wraparound)	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.com/company/product-security/bulletins/august-2021-bulletin	H-QUA-SM62-170921/1605

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 Wraparound)	08-Sep-21	10	Integer underflow can occur due to improper 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.com/company/product-security/bulletins/august-2021-bulletin	H-QUA-SM62-170921/1606
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.com/company/product-security/bulletins/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 Voice & Music, Snapdragon Wearables, Snapdragon Wired	https://www.qualcomm.com/company/product-security/bulletins/august-2021-bulletin	H-QUA-SM62-170921/1608

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Infrastructure and Networking **CVE ID : CVE-2021-1972**		
sm7250					
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.com/company/product-security/bulletins/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.com/company/product-security/bulletins/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.com/company/product-security/bulletins/august-2021-bulletin	H-QUA-SM72-170921/1611

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 Wraparound)	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.com/company/product-security/bulletins/august-2021-bulletin	H-QUA-SM72-170921/1612
Integer Underflow (Wrap or Wraparound)	08-Sep-21	10	Integer underflow can occur due to improper 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.com/company/product-security/bulletins/august-2021-bulletin	H-QUA-SM72-170921/1613
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.com/company/product-security/bulletins/august-2021-bulletin	H-QUA-SM72-170921/1614

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.com/company/product-security/bulletins/august-2021-bulletin	H-QUA-SM72-170921/1615
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.com/company/product-security/bulletins/august-2021-bulletin	H-QUA-SM72-170921/1616
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	08-Sep-21	10	Possible buffer overflow due to 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 Networking **CVE ID : CVE-2021-1972**	https://www.qualcomm.com/company/product-security/bulletins/august-2021-bulletin	H-QUA-SM72-170921/1617
sm7325					

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.com/company/product-security/bulletins/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.com/company/product-security/bulletins/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.com/company/product-security/bulletins/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.com/company/product-	H-QUA-SM73-170921/1621

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 **CVE ID : CVE-2021-1930**	security/bulletins/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 Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1972**	https://www.qualcomm.com/company/product-security/bulletins/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 **CVE ID : CVE-2021-1904**	https://www.qualcomm.com/company/product-security/bulletins/august-2021-bulletin	H-QUA-WCD9-170921/1623
Loop with Unreachable	08-Sep-21	5	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/bulletins/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.com/company/product-security/bulletins/august-2021-bulletin	H-QUA-WCD9-170921/1625
Integer Underflow (Wrap or Wraparound)	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.com/company/product-security/bulletins/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-

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
(Wrap or Wraparound)			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/bulletins/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 Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1972**	https://www.qualcomm.com/company/product-security/bulletins/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.com/company/product-security/bulletins/august-2021-bulletin	H-QUA-WCD9-170921/1629

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			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.com/company/product-security/bulletins/august-2021-bulletin	H-QUA-WCD9-170921/1630
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.com/company/product-security/bulletins/august-2021-bulletin	H-QUA-WCD9-170921/1631
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.com/company/product-security/bulletins/august-2021-bulletin	H-QUA-WCD9-170921/1632
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 Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1972**	m/company/product-security/bulletins/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.com/company/product-security/bulletins/august-2021-bulletin	H-QUA-WCD9-170921/1634
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.com/company/product-security/bulletins/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 **CVE ID : CVE-2021-1916**	https://www.qualcomm.com/company/product-security/bulletins/august-2021-bulletin	H-QUA-WCD9-170921/1636
Integer Underflow (Wrap or Wraparound)	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.com/company/product-security/bulletins/august-2021-bulletin	H-QUA-WCD9-170921/1637
Integer Underflow (Wrap or Wraparound)	08-Sep-21	10	Integer underflow can occur due to improper 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.com/company/product-security/bulletins/august-2021-bulletin	H-QUA-WCD9-170921/1638

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.com/company/product-security/bulletins/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 Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1972**	https://www.qualcomm.com/company/product-security/bulletins/august-2021-bulletin	H-QUA-WCD9-170921/1640
wcd9335					
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.com/company/product-security/bulletins/august-2021-bulletin	H-QUA-WCD9-170921/1641

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 Mobile, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1972**	https://www.qualcomm.com/company/product-security/bulletins/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 **CVE ID : CVE-2021-1904**	https://www.qualcomm.com/company/product-security/bulletins/august-2021-bulletin	H-QUA-WCD9-170921/1643
Loop with Unreachable	08-Sep-21	5	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/bulletins/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.com/company/product-security/bulletins/august-2021-bulletin	H-QUA-WCD9-170921/1645
Integer Underflow (Wrap or Wraparound)	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.com/company/product-security/bulletins/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-

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
(Wrap or Wraparound)			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/bulletins/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.com/company/product-security/bulletins/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.com/company/product-security/bulletins/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.com/company/product-security/bulletins/august-	H-QUA-WCD9-170921/1650

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wearables **CVE ID : CVE-2021-1929**	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 Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1972**	https://www.qualcomm.com/company/product-security/bulletins/august-2021-bulletin	H-QUA-WCD9-170921/1651
wcd9341					
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.com/company/product-security/bulletins/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.com/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/bulletins/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.com/company/product-security/bulletins/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 Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1972**	https://www.qualcomm.com/company/product-security/bulletins/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.com/company/product-	H-QUA-WCD9-170921/1656

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/bulletins/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.com/company/product-security/bulletins/august-2021-bulletin	H-QUA-WCD9-170921/1657
Integer Underflow (Wrap or Wraparound)	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.com/company/product-security/bulletins/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.com/company/product-	H-QUA-WCD9-170921/1659

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/bulletins/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.com/company/product-security/bulletins/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 Voice & Music, Snapdragon Wearables **CVE ID : CVE-2021-1904**	https://www.qualcomm.com/company/product-security/bulletins/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.com/company/product-security/bulletins/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.com/company/product-security/bulletins/august-2021-bulletin	H-QUA-WCD9-170921/1663
Integer Underflow (Wrap or Wraparound)	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.com/company/product-security/bulletins/august-2021-bulletin	H-QUA-WCD9-170921/1664
Integer Underflow (Wrap or Wraparound)	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.com/company/product-security/bulletins/august-	H-QUA-WCD9-170921/1665

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.com/company/product-security/bulletins/august-2021-bulletin	H-QUA-WCD9-170921/1666
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.com/company/product-security/bulletins/august-2021-bulletin	H-QUA-WCD9-170921/1667
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.com/company/product-security/bulletins/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 Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1972**	m/company/product-security/bulletins/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.com/company/product-security/bulletins/august-2021-bulletin	H-QUA-WCD9-170921/1670
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.com/company/product-security/bulletins/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 **CVE ID : CVE-2021-1916**	https://www.qualcomm.com/company/product-security/bulletins/august-2021-bulletin	H-QUA-WCD9-170921/1672
Integer Underflow (Wrap or Wraparound)	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.com/company/product-security/bulletins/august-2021-bulletin	H-QUA-WCD9-170921/1673
Integer Underflow (Wrap or Wraparound)	08-Sep-21	10	Integer underflow can occur due to improper 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.com/company/product-security/bulletins/august-2021-bulletin	H-QUA-WCD9-170921/1674

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.com/company/product-security/bulletins/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 Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1972**	https://www.qualcomm.com/company/product-security/bulletins/august-2021-bulletin	H-QUA-WCD9-170921/1676
wcd9375					
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.com/company/product-security/bulletins/august-2021-bulletin	H-QUA-WCD9-170921/1677

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.com/company/product-security/bulletins/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.com/company/product-security/bulletins/august-2021-bulletin	H-QUA-WCD9-170921/1679
Integer Underflow (Wrap or Wraparound)	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.com/company/product-security/bulletins/august-2021-bulletin	H-QUA-WCD9-170921/1680

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Voice & Music, Snapdragon Wearables **CVE ID : CVE-2021-1919**		
Integer Underflow (Wrap or Wraparound)	08-Sep-21	10	Integer underflow can occur due to improper 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.com/company/product-security/bulletins/august-2021-bulletin	H-QUA-WCD9-170921/1681
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.com/company/product-security/bulletins/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.com/company/product-security/bulletins/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.com/company/	H-QUA-WCD9-

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 **CVE ID : CVE-2021-1930**	product-security/bulletins/august-2021-bulletin	170921/1684
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	08-Sep-21	10	Possible buffer overflow due to 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 Networking **CVE ID : CVE-2021-1972**	https://www.qualcomm.com/company/product-security/bulletins/august-2021-bulletin	H-QUA-WCD9-170921/1685
wcd9380					
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.com/company/product-security/bulletins/august-2021-bulletin	H-QUA-WCD9-170921/1686
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 **CVE ID : CVE-2021-1914**	qualcomm.com/company/product-security/bulletins/august-2021-bulletin	WCD9-170921/1687
Out-of-bounds Write	08-Sep-21	10	Possible buffer underflow due to lack of check for negative indices values when 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.com/company/product-security/bulletins/august-2021-bulletin	H-QUA-WCD9-170921/1688
Integer Underflow (Wrap or Wraparound)	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.com/company/product-security/bulletins/august-2021-bulletin	H-QUA-WCD9-170921/1689
Integer	08-Sep-21	10	Integer underflow can occur	https://www.	H-QUA-

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Underflow (Wrap or Wraparound)			due to improper 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.com/company/product-security/bulletins/august-2021-bulletin	WCD9-170921/1690
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.com/company/product-security/bulletins/august-2021-bulletin	H-QUA-WCD9-170921/1691
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.com/company/product-security/bulletins/august-2021-bulletin	H-QUA-WCD9-170921/1692
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.com/company/product-security/bulletins/august-2021-bulletin	H-QUA-WCD9-170921/1693

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 Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1972**	https://www.qualcomm.com/company/product-security/bulletins/august-2021-bulletin	H-QUA-WCD9-170921/1694
wcd9385					
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.com/company/product-security/bulletins/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.com/company/product-security/bull	H-QUA-WCD9-170921/1696

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.com/company/product-security/bulletins/august-2021-bulletin	H-QUA-WCD9-170921/1697
Integer Underflow (Wrap or Wraparound)	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.com/company/product-security/bulletins/august-2021-bulletin	H-QUA-WCD9-170921/1698
Integer Underflow (Wrap or Wraparound)	08-Sep-21	10	Integer underflow can occur due to improper handling of incoming RTCP packets in Snapdragon Auto, Snapdragon Compute,	https://www.qualcomm.com/company/product-security/bull	H-QUA-WCD9-170921/1699

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-2021-1920**	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.com/company/product-security/bulletins/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.com/company/product-security/bulletins/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.com/company/product-security/bulletins/august-2021-bulletin	H-QUA-WCD9-170921/1702

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 Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1972**	https://www.qualcomm.com/company/product-security/bulletins/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 Voice & Music, Snapdragon Wearables **CVE ID : CVE-2021-1904**	https://www.qualcomm.com/company/product-security/bulletins/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.com/company/product-security/bulletins/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 **CVE ID : CVE-2021-1916**	https://www.qualcomm.com/company/product-security/bulletins/august-2021-bulletin	H-QUA-WCN3-170921/1706
Integer Underflow (Wrap or Wraparound)	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.com/company/product-security/bulletins/august-2021-bulletin	H-QUA-WCN3-170921/1707
Integer Underflow (Wrap or Wraparound)	08-Sep-21	10	Integer underflow can occur 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.com/company/product-security/bulletins/august-2021-bulletin	H-QUA-WCN3-170921/1708

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.com/company/product-security/bulletins/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.com/company/product-security/bulletins/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.com/company/product-security/bulletins/august-2021-bulletin	H-QUA-WCN3-170921/1711

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 Voice & Music, Snapdragon Wearables **CVE ID : CVE-2021-1904**	https://www.qualcomm.com/company/product-security/bulletins/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.com/company/product-security/bulletins/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.com/company/product-security/bulletins/august-	H-QUA-WCN3-170921/1714

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-2021-1916**	2021-bulletin	
Integer Underflow (Wrap or Wraparound)	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.com/company/product-security/bulletins/august-2021-bulletin	H-QUA-WCN3-170921/1715
Integer Underflow (Wrap or Wraparound)	08-Sep-21	10	Integer underflow can occur due to improper 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.com/company/product-security/bulletins/august-2021-bulletin	H-QUA-WCN3-170921/1716
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.com/company/product-security/bulletins/august-2021-bulletin	H-QUA-WCN3-170921/1717

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 Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1972**	https://www.qualcomm.com/company/product-security/bulletins/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 Voice & Music, Snapdragon Wearables **CVE ID : CVE-2021-1904**	https://www.qualcomm.com/company/product-security/bulletins/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.com/company/product-	H-QUA-WCN3-170921/1720

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/bulletins/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.com/company/product-security/bulletins/august-2021-bulletin	H-QUA-WCN3-170921/1721
Integer Underflow (Wrap or Wraparound)	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.com/company/product-security/bulletins/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.com/company/product-	H-QUA-WCN3-170921/1723

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/bulletins/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.com/company/product-security/bulletins/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.com/company/product-security/bulletins/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.com/company/product-security/bulletins/august-	H-QUA-WCN3-170921/1726

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.com/company/product-security/bulletins/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.com/company/product-security/bulletins/august-2021-bulletin	H-QUA-WCN3-170921/1728
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.com/company/product-security/bulletins/august-2021-bulletin	WCN3-170921/1729
Integer Underflow (Wrap or Wraparound)	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.com/company/product-security/bulletins/august-2021-bulletin	H-QUA-WCN3-170921/1730
Integer Underflow (Wrap or Wraparound)	08-Sep-21	10	Integer underflow can occur due to improper 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.com/company/product-security/bulletins/august-2021-bulletin	H-QUA-WCN3-170921/1731
Buffer Copy without	08-Sep-21	10	Possible buffer overflow due to improper validation of	https://www.qualcomm.co	H-QUA-WCN3-

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 Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1972**	m/company/product-security/bulletins/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.com/company/product-security/bulletins/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.com/company/product-security/bulletins/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 **CVE ID : CVE-2021-1916**	https://www.qualcomm.com/company/product-security/bulletins/august-2021-bulletin	H-QUA-WCN3-170921/1735
Integer Underflow (Wrap or Wraparound)	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.com/company/product-security/bulletins/august-2021-bulletin	H-QUA-WCN3-170921/1736
Integer Underflow (Wrap or Wraparound)	08-Sep-21	10	Integer underflow can occur due to improper 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.com/company/product-security/bulletins/august-2021-bulletin	H-QUA-WCN3-170921/1737

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.com/company/product-security/bulletins/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.com/company/product-security/bulletins/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 Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and	https://www.qualcomm.com/company/product-security/bulletins/august-2021-bulletin	H-QUA-WCN3-170921/1740

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 Voice & Music, Snapdragon Wearables **CVE ID : CVE-2021-1904**	https://www.qualcomm.com/company/product-security/bulletins/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.com/company/product-security/bulletins/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.com/company/product-security/bulletins/august-2021-bulletin	H-QUA-WCN3-170921/1743

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 Wraparound)	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.com/company/product-security/bulletins/august-2021-bulletin	H-QUA-WCN3-170921/1744
Integer Underflow (Wrap or Wraparound)	08-Sep-21	10	Integer underflow can occur due to improper 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.com/company/product-security/bulletins/august-2021-bulletin	H-QUA-WCN3-170921/1745
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.com/company/product-security/bulletins/august-2021-bulletin	H-QUA-WCN3-170921/1746

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 Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1972**	https://www.qualcomm.com/company/product-security/bulletins/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.com/company/product-security/bulletins/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.com/company/product-security/bulletins/august-	H-QUA-WCN3-170921/1749

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.com/company/product-security/bulletins/august-2021-bulletin	H-QUA-WCN3-170921/1750
Integer Underflow (Wrap or Wraparound)	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.com/company/product-security/bulletins/august-2021-bulletin	H-QUA-WCN3-170921/1751
Integer Underflow (Wrap or Wraparound)	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.com/company/product-security/bulletins/august-	H-QUA-WCN3-170921/1752

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	
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.com/company/product-security/bulletins/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 Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1972**	https://www.qualcomm.com/company/product-security/bulletins/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.com/company/	H-QUA-WCN3-170921/1755

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/bulletins/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.com/company/product-security/bulletins/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.com/company/product-security/bulletins/august-2021-bulletin	H-QUA-WCN3-170921/1757
Integer	08-Sep-21	10	Integer underflow can occur	https://www.	H-QUA-

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Underflow (Wrap or Wraparound)			when 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.com/company/product-security/bulletins/august-2021-bulletin	WCN3-170921/1758
Integer Underflow (Wrap or Wraparound)	08-Sep-21	10	Integer underflow can occur due to improper 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.com/company/product-security/bulletins/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.com/company/product-security/bulletins/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.com/company/product-security/bulletins/august-	H-QUA-WCN3-170921/1761

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wearables **CVE ID : CVE-2021-1929**	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.com/company/product-security/bulletins/august-2021-bulletin	H-QUA-WCN3-170921/1762
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	08-Sep-21	10	Possible buffer overflow due to 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 Networking **CVE ID : CVE-2021-1972**	https://www.qualcomm.com/company/product-security/bulletins/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.com/company/product-security/bulletins/august-2021-bulletin	H-QUA-WCN3-170921/1764

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.com/company/product-security/bulletins/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.com/company/product-security/bulletins/august-2021-bulletin	H-QUA-WCN3-170921/1766
Integer Underflow (Wrap or Wraparound)	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.com/company/product-security/bull	H-QUA-WCN3-170921/1767

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-2021-1919**	etins/august-2021-bulletin	
Integer Underflow (Wrap or Wraparound)	08-Sep-21	10	Integer underflow can occur due to improper 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.com/company/product-security/bulletins/august-2021-bulletin	H-QUA-WCN3-170921/1768
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.com/company/product-security/bulletins/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.com/company/product-security/bulletins/august-2021-bulletin	H-QUA-WCN3-170921/1770

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.com/company/product-security/bulletins/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 Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1972**	https://www.qualcomm.com/company/product-security/bulletins/august-2021-bulletin	H-QUA-WCN3-170921/1772
wcn3980					
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.com/company/product-security/bulletins/august-2021-bulletin	H-QUA-WCN3-170921/1773

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.com/company/product-security/bulletins/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.com/company/product-security/bulletins/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.com/company/product-security/bulletins/august-2021-bulletin	H-QUA-WCN3-170921/1776

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 Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1972**	https://www.qualcomm.com/company/product-security/bulletins/august-2021-bulletin	H-QUA-WCN3-170921/1777
wcn3988					
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.com/company/product-security/bulletins/august-2021-bulletin	H-QUA-WCN3-170921/1778
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.com/company/product-security/bulletins/august-2021-bulletin	H-QUA-WCN3-170921/1779

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.com/company/product-security/bulletins/august-2021-bulletin	H-QUA-WCN3-170921/1780
Integer Underflow (Wrap or Wraparound)	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.com/company/product-security/bulletins/august-2021-bulletin	H-QUA-WCN3-170921/1781
Integer Underflow (Wrap or Wraparound)	08-Sep-21	10	Integer underflow can occur 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.com/company/product-security/bulletins/august-2021-bulletin	H-QUA-WCN3-170921/1782

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.com/company/product-security/bulletins/august-2021-bulletin	H-QUA-WCN3-170921/1783
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.com/company/product-security/bulletins/august-2021-bulletin	H-QUA-WCN3-170921/1784
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.com/company/product-security/bulletins/august-2021-bulletin	H-QUA-WCN3-170921/1785
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.com/company/product-security/bull	H-QUA-WCN3-170921/1786

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					
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.com/company/product-security/bulletins/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.com/company/product-security/bulletins/august-2021-bulletin	H-QUA-WCN3-170921/1788
Improper Restriction	08-Sep-21	3.6	Possible out of bounds read due to incorrect validation of	https://www.qualcomm.co	H-QUA-WCN3-

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/bulletins/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 Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1972**	https://www.qualcomm.com/company/product-security/bulletins/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 Voice & Music, Snapdragon Wearables **CVE ID : CVE-2021-1904**	https://www.qualcomm.com/company/product-security/bulletins/august-2021-bulletin	H-QUA-WCN3-170921/1791

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.com/company/product-security/bulletins/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.com/company/product-security/bulletins/august-2021-bulletin	H-QUA-WCN3-170921/1793
Integer Underflow (Wrap or Wraparound)	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.com/company/product-security/bulletins/august-2021-bulletin	H-QUA-WCN3-170921/1794

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Integer Underflow (Wrap or Wraparound)	08-Sep-21	10	Integer underflow can occur due to improper 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.com/company/product-security/bulletins/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.com/company/product-security/bulletins/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.com/company/product-security/bulletins/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.com/company/product-security/bulletins/august-	H-QUA-WCN3-170921/1798

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 Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1972**	https://www.qualcomm.com/company/product-security/bulletins/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 Voice & Music, Snapdragon Wearables **CVE ID : CVE-2021-1904**	https://www.qualcomm.com/company/product-security/bulletins/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.com/company/product-	H-QUA-WCN3-170921/1801

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/bulletins/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.com/company/product-security/bulletins/august-2021-bulletin	H-QUA-WCN3-170921/1802
Integer Underflow (Wrap or Wraparound)	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.com/company/product-security/bulletins/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.com/company/product-	H-QUA-WCN3-170921/1804

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/bulletins/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.com/company/product-security/bulletins/august-2021-bulletin	H-QUA-WCN3-170921/1805
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.com/company/product-security/bulletins/august-2021-bulletin	H-QUA-WCN3-170921/1806
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.com/company/product-security/bulletins/august-2021-bulletin	H-QUA-WCN3-170921/1807

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 Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1972**	https://www.qualcomm.com/company/product-security/bulletins/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.com/company/product-security/bulletins/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.com/company/product-security/bulletins/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 Voice & Music, Snapdragon Wearables **CVE ID : CVE-2021-1904**	https://www.qualcomm.com/company/product-security/bulletins/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.com/company/product-security/bulletins/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.com/company/product-	H-QUA-WCN6-170921/1813

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/bulletins/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.com/company/product-security/bulletins/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.com/company/product-security/bulletins/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 Voice & Music, Snapdragon Wearables, Snapdragon Wired	https://www.qualcomm.com/company/product-security/bulletins/august-2021-bulletin	H-QUA-WCN6-170921/1816

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Infrastructure and Networking **CVE ID : CVE-2021-1972**		
wcn6750					
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.com/company/product-security/bulletins/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.com/company/product-security/bulletins/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.com/company/product-security/bulletins/august-2021-bulletin	H-QUA-WCN6-170921/1819

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 Wraparound)	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.com/company/product-security/bulletins/august-2021-bulletin	H-QUA-WCN6-170921/1820
Integer Underflow (Wrap or Wraparound)	08-Sep-21	10	Integer underflow can occur due to improper 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.com/company/product-security/bulletins/august-2021-bulletin	H-QUA-WCN6-170921/1821
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.com/company/product-security/bulletins/august-2021-bulletin	H-QUA-WCN6-170921/1822

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.com/company/product-security/bulletins/august-2021-bulletin	H-QUA-WCN6-170921/1823
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.com/company/product-security/bulletins/august-2021-bulletin	H-QUA-WCN6-170921/1824
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	08-Sep-21	10	Possible buffer overflow due to 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 Networking **CVE ID : CVE-2021-1972**	https://www.qualcomm.com/company/product-security/bulletins/august-2021-bulletin	H-QUA-WCN6-170921/1825
wcn6850					

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.com/company/product-security/bulletins/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.com/company/product-security/bulletins/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.com/company/product-security/bulletins/august-2021-bulletin	H-QUA-WCN6-170921/1828

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2021-1916		
Integer Underflow (Wrap or Wraparound)	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.com/company/product-security/bulletins/august-2021-bulletin	H-QUA-WCN6-170921/1829
Integer Underflow (Wrap or Wraparound)	08-Sep-21	10	Integer underflow can occur due to improper 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.com/company/product-security/bulletins/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.com/company/product-security/bulletins/august-2021-bulletin	H-QUA-WCN6-170921/1831
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.com/company/product-	H-QUA-WCN6-170921/1832

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/bulletins/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.com/company/product-security/bulletins/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 Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1972**	https://www.qualcomm.com/company/product-security/bulletins/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.com/company/product-security/bull	H-QUA-WCN6-170921/1835

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.com/company/product-security/bulletins/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.com/company/product-security/bulletins/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.com/company/	H-QUA-WCN6-170921/1838

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Wraparound)			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/bulletins/august-2021-bulletin	
Integer Underflow (Wrap or Wraparound)	08-Sep-21	10	Integer underflow can occur due to improper 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.com/company/product-security/bulletins/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.com/company/product-security/bulletins/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.com/company/product-security/bulletins/august-2021-bulletin	H-QUA-WCN6-170921/1841

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.com/company/product-security/bulletins/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 Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1972**	https://www.qualcomm.com/company/product-security/bulletins/august-2021-bulletin	H-QUA-WCN6-170921/1843
wcn6855					
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.com/company/product-security/bulletins/august-2021-bulletin	H-QUA-WCN6-170921/1844

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 **CVE ID : CVE-2021-1914**	https://www.qualcomm.com/company/product-security/bulletins/august-2021-bulletin	H-QUA-WCN6-170921/1845
Out-of-bounds Write	08-Sep-21	10	Possible buffer underflow due to lack of check for negative indices values when 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.com/company/product-security/bulletins/august-2021-bulletin	H-QUA-WCN6-170921/1846
Integer Underflow (Wrap or Wraparound)	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.com/company/product-security/bulletins/august-2021-bulletin	H-QUA-WCN6-170921/1847

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 Wraparound)	08-Sep-21	10	Integer underflow can occur due to improper 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.com/company/product-security/bulletins/august-2021-bulletin	H-QUA-WCN6-170921/1848
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.com/company/product-security/bulletins/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.com/company/product-security/bulletins/august-2021-bulletin	H-QUA-WCN6-170921/1850
wcn6856					

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.com/company/product-security/bulletins/august-2021-bulletin	H-QUA-WCN6-170921/1851
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.com/company/product-security/bulletins/august-2021-bulletin	H-QUA-WCN6-170921/1852
Out-of-bounds Write	08-Sep-21	10	Possible buffer underflow due to lack of check for negative indices values when 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.com/company/product-security/bulletins/august-2021-bulletin	H-QUA-WCN6-170921/1853

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2021-1916		
Integer Underflow (Wrap or Wraparound)	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.com/company/product-security/bulletins/august-2021-bulletin	H-QUA-WCN6-170921/1854
Integer Underflow (Wrap or Wraparound)	08-Sep-21	10	Integer underflow can occur due to improper 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.com/company/product-security/bulletins/august-2021-bulletin	H-QUA-WCN6-170921/1855
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.com/company/product-security/bulletins/august-2021-bulletin	H-QUA-WCN6-170921/1856
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.com/company/product-	H-QUA-WCN6-170921/1857

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/bulletins/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.com/company/product-security/bulletins/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 Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1972**	https://www.qualcomm.com/company/product-security/bulletins/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.com/company/product-security/bull	H-QUA-WHS9-170921/1860

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.com/company/product-security/bulletins/august-2021-bulletin	H-QUA-WHS9-170921/1861
Integer Underflow (Wrap or Wraparound)	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.com/company/product-security/bulletins/august-2021-bulletin	H-QUA-WHS9-170921/1862
Integer Underflow (Wrap or Wraparound)	08-Sep-21	10	Integer underflow can occur due to improper handling of incoming RTCP packets in Snapdragon Auto, Snapdragon Compute,	https://www.qualcomm.com/company/product-security/bull	H-QUA-WHS9-170921/1863

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-2021-1920**	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.com/company/product-security/bulletins/august-2021-bulletin	H-QUA-WHS9-170921/1864
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 Voice & Music, Snapdragon Wearables **CVE ID : CVE-2021-1904**	https://www.qualcomm.com/company/product-security/bulletins/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.com/company/product-security/bulletins/august-2021-bulletin	H-QUA-WSA8-170921/1866

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.com/company/product-security/bulletins/august-2021-bulletin	H-QUA-WSA8-170921/1867
Integer Underflow (Wrap or Wraparound)	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.com/company/product-security/bulletins/august-2021-bulletin	H-QUA-WSA8-170921/1868
Integer Underflow (Wrap or Wraparound)	08-Sep-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.com/company/product-security/bulletins/august-2021-bulletin	H-QUA-WSA8-170921/1869

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.com/company/product-security/bulletins/august-2021-bulletin	H-QUA-WSA8-170921/1870
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.com/company/product-security/bulletins/august-2021-bulletin	H-QUA-WSA8-170921/1871
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.com/company/product-security/bulletins/august-2021-bulletin	H-QUA-WSA8-170921/1872

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.com/company/product-security/bulletins/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 Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1972**	https://www.qualcomm.com/company/product-security/bulletins/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.com/company/product-security/bulletins/august-2021-bulletin	H-QUA-WSA8-170921/1875

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.com/company/product-security/bulletins/august-2021-bulletin	H-QUA-WSA8-170921/1876
Out-of-bounds Write	08-Sep-21	10	Possible buffer underflow due to lack of check for negative indices values when 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.com/company/product-security/bulletins/august-2021-bulletin	H-QUA-WSA8-170921/1877
Integer Underflow (Wrap or Wraparound)	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.com/company/product-security/bulletins/august-2021-bulletin	H-QUA-WSA8-170921/1878

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Wearables **CVE ID : CVE-2021-1919**		
Integer Underflow (Wrap or Wraparound)	08-Sep-21	10	Integer underflow can occur due to improper 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.com/company/product-security/bulletins/august-2021-bulletin	H-QUA-WSA8-170921/1879
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.com/company/product-security/bulletins/august-2021-bulletin	H-QUA-WSA8-170921/1880
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.com/company/product-security/bulletins/august-2021-bulletin	H-QUA-WSA8-170921/1881
Exposure of Resource to	08-Sep-21	2.1	Lack of strict validation of bootmode can lead to	https://www.qualcomm.co	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/bulletins/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.com/company/product-security/bulletins/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 Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1972**	https://www.qualcomm.com/company/product-security/bulletins/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.com/company/	H-QUA-WSA8-170921/1885

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/bulletins/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.com/company/product-security/bulletins/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.com/company/product-security/bulletins/august-2021-bulletin	H-QUA-WSA8-170921/1887
Integer	08-Sep-21	10	Integer underflow can occur	https://www.	H-QUA-WSA8-

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Underflow (Wrap or Wraparound)			when 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.com/company/product-security/bulletins/august-2021-bulletin	170921/1888
Integer Underflow (Wrap or Wraparound)	08-Sep-21	10	Integer underflow can occur due to improper 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.com/company/product-security/bulletins/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.com/company/product-security/bulletins/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.com/company/product-security/bulletins/august-	H-QUA-WSA8-170921/1891

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wearables **CVE ID : CVE-2021-1929**	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.com/company/product-security/bulletins/august-2021-bulletin	H-QUA-WSA8-170921/1892
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	08-Sep-21	10	Possible buffer overflow due to 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 Networking **CVE ID : CVE-2021-1972**	https://www.qualcomm.com/company/product-security/bulletins/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.com/company/product-security/bulletins/august-2021-bulletin	H-QUA-WSA8-170921/1894

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.com/company/product-security/bulletins/august-2021-bulletin	H-QUA-WSA8-170921/1895
Out-of-bounds Write	08-Sep-21	10	Possible buffer underflow due to lack of check for negative indices values when 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.com/company/product-security/bulletins/august-2021-bulletin	H-QUA-WSA8-170921/1896
Integer Underflow (Wrap or Wraparound)	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.com/company/product-security/bull	H-QUA-WSA8-170921/1897

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-2021-1919**	etins/august-2021-bulletin	
Integer Underflow (Wrap or Wraparound)	08-Sep-21	10	Integer underflow can occur due to improper 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.com/company/product-security/bulletins/august-2021-bulletin	H-QUA-WSA8-170921/1898
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.com/company/product-security/bulletins/august-2021-bulletin	H-QUA-WSA8-170921/1899
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.com/company/product-security/bulletins/august-2021-bulletin	H-QUA-WSA8-170921/1900

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.com/company/product-security/bulletins/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 Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1972**	https://www.qualcomm.com/company/product-security/bulletins/august-2021-bulletin	H-QUA-WSA8-170921/1902
Samsung					
h3					
Incorrect Authorization	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

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2021-39373		
Schneider-electric					
accusine_pcsn					
Exposure of Sensitive Information to an Unauthorized 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://download.schneider-electric.com/files?p_Doc_Ref=SEVD-2021-222-05	H-SCH-ACCU-170921/1904
accusine_pcs\\+					
Exposure of Sensitive Information to an Unauthorized 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://download.schneider-electric.com/files?p_Doc_Ref=SEVD-2021-222-05	H-SCH-ACCU-170921/1905
accusine_pfv\\+					
Exposure of Sensitive Information to an Unauthorized 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://download.schneider-electric.com/files?p_Doc_Ref=SEVD-2021-222-05	H-SCH-ACCU-170921/1906

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_m340_bmxp341000					
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 EcoStruxureª Control Expert, 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), Modicon Quantum CPU (part numbers 140CPU*, all versions), Modicon Premium CPU (part	https://download.schneider-electric.com/files?p_Doc_Ref=SEVD-2021-222-04	H-SCH-MODI-170921/1907

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			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 EcoStruxureª Control Expert, 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), Modicon Quantum CPU (part numbers 140CPU*, all versions), Modicon Premium CPU (part numbers TSXP5*, all versions). **CVE ID : CVE-2021-22790**	https://download.schneider-electric.com/files?p_Doc_Ref=SEVD-2021-222-04	H-SCH-MODI-170921/1908
Out-of-bounds	02-Sep-21	4	A CWE-787: Out-of-bounds Write vulnerability that could	https://download.schneide	H-SCH-MODI-170921/1909

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 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 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). **CVE ID : CVE-2021-22791**	r-electric.com/files?p_Doc_Ref=SEVD-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	https://download.schneider-electric.com/files?p_Doc_Ref=SEVD-2021-222-04	H-SCH-MODI-170921/1910

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 EcoStruxureª Control Expert, 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), Modicon Quantum CPU (part numbers 140CPU*, all versions), Modicon Premium CPU (part numbers TSXP5*, all versions). **CVE ID : CVE-2021-22792**		
modicon_m340_bmxp342010					
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://download.schneider-electric.com/files?p_Doc_Ref=SEVD-2021-222-04	H-SCH-MODI-170921/1911

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 EcoStruxureª Control Expert, 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), 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://download.schneider-electric.com/files?p_Doc_Ref=SEVD-2021-222-04	H-SCH-MODI-170921/1912

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			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 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). **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 EcoStruxureª Control Expert, including all Unity Pro	https://download.schneider-electric.com/files?p_Doc_Ref=SEVD-2021-222-04	H-SCH-MODI-170921/1913

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			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), 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® Control Expert, including all Unity Pro versions (former name of EcoStruxure® Control Expert, all versions), PLC Simulator for EcoStruxure® Process Expert including all HDCS	https://download.schneider-electric.com/files?p_Doc_Ref=SEVD-2021-222-04	H-SCH-MODI-170921/1914

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			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). **CVE ID : CVE-2021-22792**		
modicon_m340_bmxp342020					
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® 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	https://download.schneider-electric.com/files?p_Doc_Ref=SEVD-2021-222-04	H-SCH-MODI-170921/1915

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			EcoStruxureª 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 EcoStruxureª Control Expert, 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), Modicon Quantum CPU (part numbers 140CPU*, all versions), Modicon Premium CPU (part numbers TSXP5*, all	https://download.schneider-electric.com/files?p_Doc_Ref=SEVD-2021-222-04	H-SCH-MODI-170921/1916

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			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 EcoStruxureª Control Expert, 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), Modicon Quantum CPU (part numbers 140CPU*, all versions), Modicon Premium CPU (part numbers TSXP5*, all versions). **CVE ID : CVE-2021-22791**	https://download.schneider-electric.com/files?p_Doc_Ref=SEVD-2021-222-04	H-SCH-MODI-170921/1917
NULL Pointer Dereference	02-Sep-21	5	A CWE-476: NULL Pointer Dereference vulnerability that could cause a Denial of	https://download.schneider-	H-SCH-MODI-170921/1918

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			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 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), Modicon Quantum CPU (part numbers 140CPU*, all versions), Modicon Premium CPU (part numbers TSXP5*, all versions). **CVE ID : CVE-2021-22792**	electric.com/files?p_Doc_Ref=SEVD-2021-222-04	
modicon_m340_bmxp342030					
Improper Restriction of Operations within the Bounds of a	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	https://download.schneider-electric.com/files?p_Doc_Ref=SEVD-	H-SCH-MODI-170921/1919

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 EcoStruxureª Control Expert, 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), 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	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	https://download.schneider-electric.com/files?p_Doc_Ref=SEVD-2021-222-04	H-SCH-MODI-170921/1920

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 EcoStruxureª Control Expert, 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), 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://download.schneider-electric.com/files?p_Doc_Ref=SEVD-2021-222-04	H-SCH-MODI-170921/1921

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			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 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). **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 EcoStruxureª Control Expert, including all Unity Pro	https://download.schneider-electric.com/files?p_Doc_Ref=SEVD-2021-222-04	H-SCH-MODI-170921/1922

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			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), Modicon Quantum CPU (part numbers 140CPU*, all versions), Modicon Premium CPU (part numbers TSXP5*, all versions). **CVE ID : CVE-2021-22792**		
modicon_m580_bmeh582040					
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® Control Expert, including all Unity Pro versions (former name of	https://download.schneider-electric.com/files?p_Doc_Ref=SEVD-2021-222-04	H-SCH-MODI-170921/1923

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			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). **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 EcoStruxureª Control Expert, 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,	https://download.schneider-electric.com/files?p_Doc_Ref=SEVD-2021-222-04	H-SCH-MODI-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 EcoStruxureª Control Expert, 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), Modicon Quantum CPU (part numbers 140CPU*, all versions), Modicon Premium CPU (part numbers TSXP5*, all	https://download.schneider-electric.com/files?p_Doc_Ref=SEVD-2021-222-04	H-SCH-MODI-170921/1925

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 EcoStruxureª Control Expert, 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), Modicon Quantum CPU (part numbers 140CPU*, all versions), Modicon Premium CPU (part numbers TSXP5*, all versions). **CVE ID : CVE-2021-22792**	https://download.schneider-electric.com/files?p_Doc_Ref=SEVD-2021-222-04	H-SCH-MODI-170921/1926
modicon_m580_bmeh582040c					

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
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 EcoStruxureª Control Expert, 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), Modicon Quantum CPU (part numbers 140CPU*, all versions), Modicon Premium CPU (part numbers TSXP5*, all versions). **CVE ID : CVE-2021-22789**	https://download.schneider-electric.com/files?p_Doc_Ref=SEVD-2021-222-04	H-SCH-MODI-170921/1927
Out-of-bounds	02-Sep-21	4	A CWE-125: Out-of-bounds Read vulnerability that could cause a Denial of Service on	https://download.schneider-	H-SCH-MODI-170921/1928

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 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 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). **CVE ID : CVE-2021-22790**	electric.com/files?p_Doc_Ref=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	https://download.schneider-electric.com/files?p_Doc_Ref=SEVD-2021-222-04	H-SCH-MODI-170921/1929

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 EcoStruxureª Control Expert, 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), 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	https://download.schneider-electric.com/files?p_Doc_Ref=SEVD-2021-222-04	H-SCH-MODI-170921/1930

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			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 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). **CVE ID : CVE-2021-22792**		
modicon_m580_bmeh582040s					
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://download.schneider-electric.com/files?p_Doc_Ref=SEVD-2021-222-04	H-SCH-MODI-170921/1931

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			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 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). **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 EcoStruxureª Control Expert, including all Unity Pro versions (former name of	https://download.schneider-electric.com/files?p_Doc_Ref=SEVD-2021-222-04	H-SCH-MODI-170921/1932

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			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). **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 EcoStruxureª Control Expert, 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,	https://download.schneider-electric.com/files?p_Doc_Ref=SEVD-2021-222-04	H-SCH-MODI-170921/1933

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 EcoStruxureª Control Expert, 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), Modicon Quantum CPU (part numbers 140CPU*, all versions), Modicon Premium CPU (part numbers TSXP5*, all	https://download.schneider-electric.com/files?p_Doc_Ref=SEVD-2021-222-04	H-SCH-MODI-170921/1934

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 EcoStruxureª Control Expert, 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), Modicon Quantum CPU (part numbers 140CPU*, all versions), Modicon Premium CPU (part numbers TSXP5*, all versions).	https://download.schneider-electric.com/files?p_Doc_Ref=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 EcoStruxureª Control Expert, 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), Modicon Quantum CPU (part numbers 140CPU*, all versions), Modicon Premium CPU (part numbers TSXP5*, all versions). **CVE ID : CVE-2021-22790**	https://download.schneider-electric.com/files?p_Doc_Ref=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://download.schneider-electric.com/f	H-SCH-MODI-170921/1937

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 EcoStruxureª Control Expert, 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), Modicon Quantum CPU (part numbers 140CPU*, all versions), Modicon Premium CPU (part numbers TSXP5*, all versions). **CVE ID : CVE-2021-22791**	iles?p_Doc_Ref=SEVD-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*,	https://download.schneider-electric.com/files?p_Doc_Ref=SEVD-2021-222-04	H-SCH-MODI-170921/1938

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 EcoStruxureª Control Expert, 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), Modicon Quantum CPU (part numbers 140CPU*, all versions), Modicon Premium CPU (part numbers TSXP5*, all versions). **CVE ID : CVE-2021-22792**		
modicon_m580_bmeh584040c					
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://download.schneider-electric.com/files?p_Doc_Ref=SEVD-2021-222-04	H-SCH-MODI-170921/1939

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 EcoStruxureª Control Expert, 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), 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	https://download.schneider-electric.com/files?p_Doc_Ref=SEVD-2021-222-04	H-SCH-MODI-170921/1940

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			(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 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). **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 EcoStruxureª Control Expert, including all Unity Pro versions (former name of EcoStruxureª Control Expert,	https://download.schneider-electric.com/files?p_Doc_Ref=SEVD-2021-222-04	H-SCH-MODI-170921/1941

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://download.schneider-electric.com/files?p_Doc_Ref=SEVD-2021-222-04	H-SCH-MODI-170921/1942

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_m580_bmeh584040s					
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 EcoStruxureª Control Expert, 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), Modicon	https://download.schneider-electric.com/files?p_Doc_Ref=SEVD-2021-222-04	H-SCH-MODI-170921/1943

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://download.schneider-electric.com/files?p_Doc_Ref=SEVD-2021-222-04	H-SCH-MODI-170921/1944

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 EcoStruxureª Control Expert, 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), Modicon Quantum CPU (part numbers 140CPU*, all versions), Modicon Premium CPU (part numbers TSXP5*, all versions). **CVE ID : CVE-2021-22791**	https://download.schneider-electric.com/files?p_Doc_Ref=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://download.schneider-electric.com/f	H-SCH-MODI-170921/1946

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 EcoStruxureª Control Expert, 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), Modicon Quantum CPU (part numbers 140CPU*, all versions), Modicon Premium CPU (part numbers TSXP5*, all versions). **CVE ID : CVE-2021-22792**	iles?p_Doc_Ref=SEVD-2021-222-04	
modicon_m580_bmeh586040					
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://download.schneider-electric.com/files?p_Doc_Ref=SEVD-2021-222-04	H-SCH-MODI-170921/1947

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 EcoStruxureª Control Expert, 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), 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://download.schneider-electric.com/files?p_Doc_Ref=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™ 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), 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	https://download.schneider-electric.com/files?p_Doc_Ref=SEVD-2021-222-04	H-SCH-MODI-170921/1949

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			(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 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). **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 EcoStruxureª Control Expert, including all Unity Pro versions (former name of	https://download.schneider-electric.com/files?p_Doc_Ref=SEVD-2021-222-04	H-SCH-MODI-170921/1950

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			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). **CVE ID : CVE-2021-22792**		
modicon_m580_bmeh586040c					
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 EcoStruxureª Control Expert, including all Unity Pro versions (former name of EcoStruxureª Control Expert,	https://download.schneider-electric.com/files?p_Doc_Ref=SEVD-2021-222-04	H-SCH-MODI-170921/1951

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://download.schneider-electric.com/files?p_Doc_Ref=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://download.schneider-electric.com/files?p_Doc_Ref=SEVD-2021-222-04	H-SCH-MODI-170921/1953

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 EcoStruxureª Control Expert, 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), Modicon Quantum CPU (part numbers 140CPU*, all versions), Modicon Premium CPU (part numbers TSXP5*, all versions). **CVE ID : CVE-2021-22792**	https://download.schneider-electric.com/files?p_Doc_Ref=SEVD-2021-222-04	H-SCH-MODI-170921/1954
modicon_m580_bmeh586040s					
Improper Restriction	02-Sep-21	4	A CWE-119: Improper Restriction of Operations	https://download.schneide	H-SCH-MODI-170921/1955

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
of Operations within the Bounds of a Memory Buffer			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 EcoStruxureª Control Expert, 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), Modicon Quantum CPU (part numbers 140CPU*, all versions), Modicon Premium CPU (part numbers TSXP5*, all versions). **CVE ID : CVE-2021-22789**	r-electric.com/files?p_Doc_Ref=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://download.schneider-electric.com/files?p_Doc_Re	H-SCH-MODI-170921/1956

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). **CVE ID : CVE-2021-22790**	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://download.schneider-electric.com/files?p_Doc_Ref=SEVD-2021-222-04	H-SCH-MODI-170921/1957

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			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 of 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). **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	https://download.schneider-electric.com/files?p_Doc_Ref=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 EcoStruxureª Control Expert, 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), 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://download.schneider-electric.com/files?p_Doc_Ref=SEVD-2021-222-04	H-SCH-MODI-170921/1959

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			versions), PLC Simulator for EcoStruxureª Control Expert, 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), 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 EcoStruxureª Control Expert, including all Unity Pro versions (former name of EcoStruxureª Control Expert, all versions), PLC Simulator	https://download.schneider-electric.com/files?p_Doc_Ref=SEVD-2021-222-04	H-SCH-MODI-170921/1960

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			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). **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™ 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), Modicon Quantum CPU (part numbers	https://download.schneider-electric.com/files?p_Doc_Ref=SEVD-2021-222-04	H-SCH-MODI-170921/1961

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			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 EcoStruxureª Control Expert, 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), Modicon Quantum CPU (part numbers 140CPU*, all versions), Modicon Premium CPU (part numbers TSXP5*, all versions).	https://download.schneider-electric.com/files?p_Doc_Ref=SEVD-2021-222-04	H-SCH-MODI-170921/1962

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2021-22792		
modicon_m580_bmep581020h					
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 EcoStruxureª Control Expert, 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), Modicon Quantum CPU (part numbers 140CPU*, all versions), Modicon Premium CPU (part numbers TSXP5*, all versions). **CVE ID : CVE-2021-22789**	https://download.schneider-electric.com/files?p_Doc_Ref=SEVD-2021-222-04	H-SCH-MODI-170921/1963

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 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 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). **CVE ID : CVE-2021-22790**	https://download.schneider-electric.com/files?p_Doc_Ref=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://download.schneider-electric.com/files?p_Doc_Ref=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 EcoStruxureª Control Expert, 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), Modicon Quantum CPU (part numbers 140CPU*, all versions), Modicon Premium CPU (part numbers TSXP5*, all versions). **CVE ID : CVE-2021-22791**	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://download.schneider-electric.com/files?p_Doc_Ref=SEVD-2021-222-04	H-SCH-MODI-170921/1966

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 EcoStruxureª Control Expert, 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), Modicon Quantum CPU (part numbers 140CPU*, all versions), Modicon Premium CPU (part numbers TSXP5*, all versions). **CVE ID : CVE-2021-22792**		
modicon_m580_bmep582020					
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://download.schneider-electric.com/files?p_Doc_Ref=SEVD-2021-222-04	H-SCH-MODI-170921/1967

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 EcoStruxureª Control Expert, 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), 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	https://download.schneider-electric.com/files?p_Doc_Ref=SEVD-2021-222-04	H-SCH-MODI-170921/1968

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			EcoStruxureª Control Expert, 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), 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 EcoStruxureª Control Expert, including all Unity Pro versions (former name of EcoStruxureª Control Expert, all versions), PLC Simulator for EcoStruxureª Process	https://download.schneider-electric.com/files?p_Doc_Ref=SEVD-2021-222-04	H-SCH-MODI-170921/1969

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://download.schneider-electric.com/files?p_Doc_Ref=SEVD-2021-222-04	H-SCH-MODI-170921/1970

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			140CPU*, all versions), Modicon Premium CPU (part numbers TSXP5*, all versions). **CVE ID : CVE-2021-22792**		
modicon_m580_bmep582020h					
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 EcoStruxureª Control Expert, 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), Modicon Quantum CPU (part numbers 140CPU*, all versions),	https://download.schneider-electric.com/files?p_Doc_Ref=SEVD-2021-222-04	H-SCH-MODI-180921/1971

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			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 EcoStruxureª Control Expert, 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), Modicon Quantum CPU (part numbers 140CPU*, all versions), Modicon Premium CPU (part numbers TSXP5*, all versions). **CVE ID : CVE-2021-22790**	https://download.schneider-electric.com/files?p_Doc_Ref=SEVD-2021-222-04	H-SCH-MODI-180921/1972
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 EcoStruxureª Control Expert, 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), Modicon Quantum CPU (part numbers 140CPU*, all versions), Modicon Premium CPU (part numbers TSXP5*, all versions). **CVE ID : CVE-2021-22791**	load.schneider-electric.com/files?p_Doc_Ref=SEVD-2021-222-04	180921/1973
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	https://download.schneider-electric.com/files?p_Doc_Ref=SEVD-	H-SCH-MODI-180921/1974

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 EcoStruxureª Control Expert, 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), 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_m580_bmep582040					
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://download.schneider-electric.com/files?p_Doc_Ref=SEVD-2021-222-04	H-SCH-MODI-180921/1975

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 EcoStruxureª Control Expert, 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), 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	https://download.schneider-electric.com/files?p_Doc_Ref=SEVD-2021-222-04	H-SCH-MODI-180921/1976

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			(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 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). **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 EcoStruxureª Control Expert,	https://download.schneider-electric.com/files?p_Doc_Ref=SEVD-2021-222-04	H-SCH-MODI-180921/1977

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			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), 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 EcoStruxureª Control Expert, including all Unity Pro versions (former name of EcoStruxureª Control Expert, all versions), PLC Simulator for EcoStruxureª Process	https://download.schneider-electric.com/files?p_Doc_Ref=SEVD-2021-222-04	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_m580_bmep582040h					
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://download.schneider-electric.com/files?p_Doc_Ref=SEVD-2021-222-04	H-SCH-MODI-180921/1979

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			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). **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® 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), Modicon Quantum CPU (part numbers 140CPU*, all versions), Modicon Premium CPU (part	https://download.schneider-electric.com/files?p_Doc_Ref=SEVD-2021-222-04	H-SCH-MODI-180921/1980

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 EcoStruxureª Control Expert, 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), Modicon Quantum CPU (part numbers 140CPU*, all versions), Modicon Premium CPU (part numbers TSXP5*, all versions). **CVE ID : CVE-2021-22791**	https://download.schneider-electric.com/files?p_Doc_Ref=SEVD-2021-222-04	H-SCH-MODI-180921/1981
NULL Pointer	02-Sep-21	5	A CWE-476: NULL Pointer Dereference vulnerability	https://download.schneide	H-SCH-MODI-180921/1982

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 EcoStruxureª Control Expert, 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), Modicon Quantum CPU (part numbers 140CPU*, all versions), Modicon Premium CPU (part numbers TSXP5*, all versions). **CVE ID : CVE-2021-22792**	r-electric.com/files?p_Doc_Ref=SEVD-2021-222-04	
modicon_m580_bmep582040s					
Improper Restriction of Operations within the	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	https://download.schneider-electric.com/files?p_Doc_Re	H-SCH-MODI-180921/1983

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 EcoStruxureª Control Expert, 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), Modicon Quantum CPU (part numbers 140CPU*, all versions), Modicon Premium CPU (part numbers TSXP5*, all versions). **CVE ID : CVE-2021-22789**	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://download.schneider-electric.com/files?p_Doc_Ref=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 EcoStruxureª Control Expert, 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), 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	https://download.schneider-electric.com/files?p_Doc_Ref=SEVD-2021-222-04	H-SCH-MODI-180921/1985

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			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 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). **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 EcoStruxureª Control Expert,	https://download.schneider-electric.com/files?p_Doc_Ref=SEVD-2021-222-04	H-SCH-MODI-180921/1986

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_m580_bmep583020					
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://download.schneider-electric.com/files?p_Doc_Ref=SEVD-2021-222-04	H-SCH-MODI-180921/1987

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			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), 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 EcoStruxureª Control Expert, 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	https://download.schneider-electric.com/files?p_Doc_Ref=SEVD-2021-222-04	H-SCH-MODI-180921/1988

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			EcoStruxureª 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 EcoStruxureª Control Expert, 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), Modicon Quantum CPU (part numbers 140CPU*, all versions), Modicon Premium CPU (part numbers TSXP5*, all	https://download.schneider-electric.com/files?p_Doc_Ref=SEVD-2021-222-04	H-SCH-MODI-180921/1989

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 EcoStruxureª Control Expert, 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), Modicon Quantum CPU (part numbers 140CPU*, all versions), Modicon Premium CPU (part numbers TSXP5*, all versions). **CVE ID : CVE-2021-22792**	https://download.schneider-electric.com/files?p_Doc_Ref=SEVD-2021-222-04	H-SCH-MODI-180921/1990
modicon_m580_bmep583040					

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
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 EcoStruxureª Control Expert, 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), Modicon Quantum CPU (part numbers 140CPU*, all versions), Modicon Premium CPU (part numbers TSXP5*, all versions). **CVE ID : CVE-2021-22789**	https://download.schneider-electric.com/files?p_Doc_Ref=SEVD-2021-222-04	H-SCH-MODI-180921/1991
Out-of-bounds	02-Sep-21	4	A CWE-125: Out-of-bounds Read vulnerability that could cause a Denial of Service on	https://download.schneider-	H-SCH-MODI-180921/1992

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 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 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). **CVE ID : CVE-2021-22790**	electric.com/files?p_Doc_Ref=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	https://download.schneider-electric.com/files?p_Doc_Ref=SEVD-2021-222-04	H-SCH-MODI-180921/1993

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 EcoStruxureª Control Expert, 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), 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	https://download.schneider-electric.com/files?p_Doc_Ref=SEVD-2021-222-04	H-SCH-MODI-180921/1994

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			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 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). **CVE ID : CVE-2021-22792**		
modicon_m580_bmep584020					
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://download.schneider-electric.com/files?p_Doc_Ref=SEVD-2021-222-04	H-SCH-MODI-180921/1995

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			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 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). **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 EcoStruxureª Control Expert, including all Unity Pro versions (former name of	https://download.schneider-electric.com/files?p_Doc_Ref=SEVD-2021-222-04	H-SCH-MODI-180921/1996

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			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). **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 EcoStruxureª Control Expert, 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,	https://download.schneider-electric.com/files?p_Doc_Ref=SEVD-2021-222-04	H-SCH-MODI-180921/1997

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 EcoStruxureª Control Expert, 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), Modicon Quantum CPU (part numbers 140CPU*, all versions), Modicon Premium CPU (part numbers TSXP5*, all	https://download.schneider-electric.com/files?p_Doc_Ref=SEVD-2021-222-04	H-SCH-MODI-180921/1998

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			versions). **CVE ID : CVE-2021-22792**		
modicon_m580_bmep584040					
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 EcoStruxureª Control Expert, 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), Modicon Quantum CPU (part numbers 140CPU*, all versions), Modicon Premium CPU (part numbers TSXP5*, all versions).	https://download.schneider-electric.com/files?p_Doc_Ref=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 EcoStruxureª Control Expert, 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), Modicon Quantum CPU (part numbers 140CPU*, all versions), Modicon Premium CPU (part numbers TSXP5*, all versions). **CVE ID : CVE-2021-22790**	https://download.schneider-electric.com/files?p_Doc_Ref=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://download.schneider-electric.com/f	H-SCH-MODI-180921/2001

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 EcoStruxureª Control Expert, 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), Modicon Quantum CPU (part numbers 140CPU*, all versions), Modicon Premium CPU (part numbers TSXP5*, all versions). **CVE ID : CVE-2021-22791**	iles?p_Doc_Ref=SEVD-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*,	https://download.schneider-electric.com/files?p_Doc_Ref=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 EcoStruxureª Control Expert, 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), Modicon Quantum CPU (part numbers 140CPU*, all versions), Modicon Premium CPU (part numbers TSXP5*, all versions). **CVE ID : CVE-2021-22792**		
modicon_m580_bmep584040s					
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://download.schneider-electric.com/files?p_Doc_Ref=SEVD-2021-222-04	H-SCH-MODI-180921/2003

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 EcoStruxureª Control Expert, 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), 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	https://download.schneider-electric.com/files?p_Doc_Ref=SEVD-2021-222-04	H-SCH-MODI-180921/2004

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			(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 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). **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 EcoStruxureª Control Expert, including all Unity Pro versions (former name of EcoStruxureª Control Expert,	https://download.schneider-electric.com/files?p_Doc_Ref=SEVD-2021-222-04	H-SCH-MODI-180921/2005

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://download.schneider-electric.com/files?p_Doc_Ref=SEVD-2021-222-04	H-SCH-MODI-180921/2006

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_m580_bmep585040					
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 EcoStruxureª Control Expert, 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), Modicon	https://download.schneider-electric.com/files?p_Doc_Ref=SEVD-2021-222-04	H-SCH-MODI-180921/2007

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://download.schneider-electric.com/files?p_Doc_Ref=SEVD-2021-222-04	H-SCH-MODI-180921/2008

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 EcoStruxureª Control Expert, 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), Modicon Quantum CPU (part numbers 140CPU*, all versions), Modicon Premium CPU (part numbers TSXP5*, all versions). **CVE ID : CVE-2021-22791**	https://download.schneider-electric.com/files?p_Doc_Ref=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://download.schneider-electric.com/f	H-SCH-MODI-180921/2010

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 EcoStruxureª Control Expert, 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), Modicon Quantum CPU (part numbers 140CPU*, all versions), Modicon Premium CPU (part numbers TSXP5*, all versions). **CVE ID : CVE-2021-22792**	iles?p_Doc_Ref=SEVD-2021-222-04	
modicon_m580_bmep585040c					
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://download.schneider-electric.com/files?p_Doc_Ref=SEVD-2021-222-04	H-SCH-MODI-180921/2011

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 EcoStruxureª Control Expert, 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), 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://download.schneider-electric.com/files?p_Doc_Ref=SEVD-2021-222-04	H-SCH-MODI-180921/2012

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 Momentum Ethernet CPU	https://download.schneider-electric.com/files?p_Doc_Ref=SEVD-2021-222-04	H-SCH-MODI-180921/2013

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			(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 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). **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 EcoStruxureª Control Expert, including all Unity Pro versions (former name of	https://download.schneider-electric.com/files?p_Doc_Ref=SEVD-2021-222-04	H-SCH-MODI-180921/2014

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			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). **CVE ID : CVE-2021-22792**		
modicon_m580_bmep586040					
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 EcoStruxureª Control Expert, including all Unity Pro versions (former name of EcoStruxureª Control Expert,	https://download.schneider-electric.com/files?p_Doc_Ref=SEVD-2021-222-04	H-SCH-MODI-180921/2015

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://download.schneider-electric.com/files?p_Doc_Ref=SEVD-2021-222-04	H-SCH-MODI-180921/2016

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://download.schneider-electric.com/files?p_Doc_Ref=SEVD-2021-222-04	H-SCH-MODI-180921/2017

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 EcoStruxureª Control Expert, 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), Modicon Quantum CPU (part numbers 140CPU*, all versions), Modicon Premium CPU (part numbers TSXP5*, all versions). **CVE ID : CVE-2021-22792**	https://download.schneider-electric.com/files?p_Doc_Ref=SEVD-2021-222-04	H-SCH-MODI-180921/2018
modicon_m580_bmep586040c					
Improper Restriction	02-Sep-21	4	A CWE-119: Improper Restriction of Operations	https://download.schneide	H-SCH-MODI-180921/2019

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
of Operations within the Bounds of a Memory Buffer			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 EcoStruxureª Control Expert, 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), Modicon Quantum CPU (part numbers 140CPU*, all versions), Modicon Premium CPU (part numbers TSXP5*, all versions). **CVE ID : CVE-2021-22789**	r-electric.com/files?p_Doc_Ref=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://download.schneider-electric.com/files?p_Doc_Re	H-SCH-MODI-180921/2020

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 EcoStruxureª Control Expert, 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), Modicon Quantum CPU (part numbers 140CPU*, all versions), Modicon Premium CPU (part numbers TSXP5*, all versions). **CVE ID : CVE-2021-22790**	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://download.schneider-electric.com/files?p_Doc_Ref=SEVD-2021-222-04	H-SCH-MODI-180921/2021

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			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 of 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). **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	https://download.schneider-electric.com/files?p_Doc_Ref=SEVD-2021-222-04	H-SCH-MODI-180921/2022

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			(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 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). **CVE ID : CVE-2021-22792**		
modicon_mc80_bmkc8020301					
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://download.schneider-electric.com/files?p_Doc_Ref=SEVD-2021-222-04	H-SCH-MODI-180921/2023

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			versions), PLC Simulator for EcoStruxureª Control Expert, 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), 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 EcoStruxureª Control Expert, including all Unity Pro versions (former name of EcoStruxureª Control Expert, all versions), PLC Simulator	https://download.schneider-electric.com/files?p_Doc_Ref=SEVD-2021-222-04	H-SCH-MODI-180921/2024

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			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, all versions), Modicon Quantum CPU (part numbers	https://download.schneider-electric.com/files?p_Doc_Ref=SEVD-2021-222-04	H-SCH-MODI-180921/2025

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			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 EcoStruxureª Control Expert, 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), Modicon Quantum CPU (part numbers 140CPU*, all versions), Modicon Premium CPU (part numbers TSXP5*, all versions).	https://download.schneider-electric.com/files?p_Doc_Ref=SEVD-2021-222-04	H-SCH-MODI-180921/2026

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2021-22792		
modicon_mc80_bmkc8020310					
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 EcoStruxureª Control Expert, 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), Modicon Quantum CPU (part numbers 140CPU*, all versions), Modicon Premium CPU (part numbers TSXP5*, all versions). **CVE ID : CVE-2021-22789**	https://download.schneider-electric.com/files?p_Doc_Ref=SEVD-2021-222-04	H-SCH-MODI-180921/2027

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 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 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). **CVE ID : CVE-2021-22790**	https://download.schneider-electric.com/files?p_Doc_Ref=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://download.schneider-electric.com/files?p_Doc_Ref=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 EcoStruxureª Control Expert, 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), Modicon Quantum CPU (part numbers 140CPU*, all versions), Modicon Premium CPU (part numbers TSXP5*, all versions). **CVE ID : CVE-2021-22791**	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://download.schneider-electric.com/files?p_Doc_Ref=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 EcoStruxureª Control Expert, 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), Modicon Quantum CPU (part numbers 140CPU*, all versions), Modicon Premium CPU (part numbers TSXP5*, all versions). **CVE ID : CVE-2021-22792**		
modicon_mc80_bmkc8030311					
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://download.schneider-electric.com/files?p_Doc_Ref=SEVD-2021-222-04	H-SCH-MODI-180921/2031

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 EcoStruxureª Control Expert, 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), 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	https://download.schneider-electric.com/files?p_Doc_Ref=SEVD-2021-222-04	H-SCH-MODI-180921/2032

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			EcoStruxureª Control Expert, 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), 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 EcoStruxureª Control Expert, including all Unity Pro versions (former name of EcoStruxureª Control Expert, all versions), PLC Simulator for EcoStruxureª Process	https://download.schneider-electric.com/files?p_Doc_Ref=SEVD-2021-222-04	H-SCH-MODI-180921/2033

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://download.schneider-electric.com/files?p_Doc_Ref=SEVD-2021-222-04	H-SCH-MODI-180921/2034

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			140CPU*, all versions), Modicon Premium CPU (part numbers TSXP5*, all versions). **CVE ID : CVE-2021-22792**		
modicon_momentum_171cbu78090					
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 EcoStruxureª Control Expert, 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), Modicon Quantum CPU (part numbers 140CPU*, all versions),	https://download.schneider-electric.com/files?p_Doc_Ref=SEVD-2021-222-04	H-SCH-MODI-180921/2035

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			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 EcoStruxureª Control Expert, 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), Modicon Quantum CPU (part numbers 140CPU*, all versions), Modicon Premium CPU (part numbers TSXP5*, all versions). **CVE ID : CVE-2021-22790**	https://download.schneider-electric.com/files?p_Doc_Ref=SEVD-2021-222-04	H-SCH-MODI-180921/2036
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 EcoStruxureª Control Expert, 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), Modicon Quantum CPU (part numbers 140CPU*, all versions), Modicon Premium CPU (part numbers TSXP5*, all versions). **CVE ID : CVE-2021-22791**	load.schneider-electric.com/files?p_Doc_Ref=SEVD-2021-222-04	180921/2037
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	https://download.schneider-electric.com/files?p_Doc_Ref=SEVD-	H-SCH-MODI-180921/2038

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 EcoStruxureª Control Expert, 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), 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_momentum_171cbu98090					
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://download.schneider-electric.com/files?p_Doc_Ref=SEVD-2021-222-04	H-SCH-MODI-180921/2039

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 EcoStruxureª Control Expert, 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), 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	https://download.schneider-electric.com/files?p_Doc_Ref=SEVD-2021-222-04	H-SCH-MODI-180921/2040

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			(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 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). **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 EcoStruxureª Control Expert,	https://download.schneider-electric.com/files?p_Doc_Ref=SEVD-2021-222-04	H-SCH-MODI-180921/2041

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			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), 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 EcoStruxureª Control Expert, including all Unity Pro versions (former name of EcoStruxureª Control Expert, all versions), PLC Simulator for EcoStruxureª Process	https://download.schneider-electric.com/files?p_Doc_Ref=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_momentum_171cbu98091					
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://download.schneider-electric.com/files?p_Doc_Ref=SEVD-2021-222-04	H-SCH-MODI-180921/2043

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			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). **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® 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), Modicon Quantum CPU (part numbers 140CPU*, all versions), Modicon Premium CPU (part	https://download.schneider-electric.com/files?p_Doc_Ref=SEVD-2021-222-04	H-SCH-MODI-180921/2044

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 EcoStruxureª Control Expert, 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), Modicon Quantum CPU (part numbers 140CPU*, all versions), Modicon Premium CPU (part numbers TSXP5*, all versions). **CVE ID : CVE-2021-22791**	https://download.schneider-electric.com/files?p_Doc_Ref=SEVD-2021-222-04	H-SCH-MODI-180921/2045
NULL Pointer	02-Sep-21	5	A CWE-476: NULL Pointer Dereference vulnerability	https://download.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 EcoStruxureª Control Expert, 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), Modicon Quantum CPU (part numbers 140CPU*, all versions), Modicon Premium CPU (part numbers TSXP5*, all versions). **CVE ID : CVE-2021-22792**	r-electric.com/files?p_Doc_Ref=SEVD-2021-222-04	
modicon_premium_tsxp57_1634m					
Improper Restriction of Operations within the	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	https://download.schneider-electric.com/files?p_Doc_Re	H-SCH-MODI-180921/2047

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 EcoStruxureª Control Expert, 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), Modicon Quantum CPU (part numbers 140CPU*, all versions), Modicon Premium CPU (part numbers TSXP5*, all versions). **CVE ID : CVE-2021-22789**	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://download.schneider-electric.com/files?p_Doc_Ref=SEVD-2021-222-04	H-SCH-MODI-180921/2048

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 EcoStruxureª Control Expert, 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), 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	https://download.schneider-electric.com/files?p_Doc_Ref=SEVD-2021-222-04	H-SCH-MODI-180921/2049

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			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 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). **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 EcoStruxureª Control Expert,	https://download.schneider-electric.com/files?p_Doc_Ref=SEVD-2021-222-04	H-SCH-MODI-180921/2050

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_premium_tsxp57_2634m					
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://download.schneider-electric.com/files?p_Doc_Ref=SEVD-2021-222-04	H-SCH-MODI-180921/2051

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			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), 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® 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	https://download.schneider-electric.com/files?p_Doc_Ref=SEVD-2021-222-04	H-SCH-MODI-180921/2052

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			EcoStruxureª 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 EcoStruxureª Control Expert, 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), Modicon Quantum CPU (part numbers 140CPU*, all versions), Modicon Premium CPU (part numbers TSXP5*, all	https://download.schneider-electric.com/files?p_Doc_Ref=SEVD-2021-222-04	H-SCH-MODI-180921/2053

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 EcoStruxureª Control Expert, 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), Modicon Quantum CPU (part numbers 140CPU*, all versions), Modicon Premium CPU (part numbers TSXP5*, all versions). **CVE ID : CVE-2021-22792**	https://download.schneider-electric.com/files?p_Doc_Ref=SEVD-2021-222-04	H-SCH-MODI-180921/2054
modicon_premium_tsxp57_2834m					

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
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 EcoStruxureª Control Expert, 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), Modicon Quantum CPU (part numbers 140CPU*, all versions), Modicon Premium CPU (part numbers TSXP5*, all versions). **CVE ID : CVE-2021-22789**	https://download.schneider-electric.com/files?p_Doc_Ref=SEVD-2021-222-04	H-SCH-MODI-180921/2055
Out-of-bounds	02-Sep-21	4	A CWE-125: Out-of-bounds Read vulnerability that could cause a Denial of Service on	https://download.schneider-	H-SCH-MODI-180921/2056

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 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 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). **CVE ID : CVE-2021-22790**	electric.com/files?p_Doc_Ref=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	https://download.schneider-electric.com/files?p_Doc_Ref=SEVD-2021-222-04	H-SCH-MODI-180921/2057

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 EcoStruxureª Control Expert, 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), 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	https://download.schneider-electric.com/files?p_Doc_Ref=SEVD-2021-222-04	H-SCH-MODI-180921/2058

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			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 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). **CVE ID : CVE-2021-22792**		
modicon_premium_tsxp57_454m					
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://download.schneider-electric.com/files?p_Doc_Ref=SEVD-2021-222-04	H-SCH-MODI-180921/2059

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			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 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). **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 EcoStruxureª Control Expert, including all Unity Pro versions (former name of	https://download.schneider-electric.com/files?p_Doc_Ref=SEVD-2021-222-04	H-SCH-MODI-180921/2060

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			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). **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 EcoStruxureª Control Expert, 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,	https://download.schneider-electric.com/files?p_Doc_Ref=SEVD-2021-222-04	H-SCH-MODI-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 EcoStruxureª Control Expert, 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), Modicon Quantum CPU (part numbers 140CPU*, all versions), Modicon Premium CPU (part numbers TSXP5*, all	https://download.schneider-electric.com/files?p_Doc_Ref=SEVD-2021-222-04	H-SCH-MODI-180921/2062

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			versions). **CVE ID : CVE-2021-22792**		
modicon_premium_tsxp57_4634m					
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 EcoStruxureª Control Expert, 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), Modicon Quantum CPU (part numbers 140CPU*, all versions), Modicon Premium CPU (part numbers TSXP5*, all versions).	https://download.schneider-electric.com/files?p_Doc_Ref=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 EcoStruxureª Control Expert, 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), Modicon Quantum CPU (part numbers 140CPU*, all versions), Modicon Premium CPU (part numbers TSXP5*, all versions). **CVE ID : CVE-2021-22790**	https://download.schneider-electric.com/files?p_Doc_Ref=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://download.schneider-electric.com/f	H-SCH-MODI-180921/2065

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 EcoStruxureª Control Expert, 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), Modicon Quantum CPU (part numbers 140CPU*, all versions), Modicon Premium CPU (part numbers TSXP5*, all versions). **CVE ID : CVE-2021-22791**	iles?p_Doc_Ref=SEVD-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*,	https://download.schneider-electric.com/files?p_Doc_Ref=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 EcoStruxureª Control Expert, 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), Modicon Quantum CPU (part numbers 140CPU*, all versions), Modicon Premium CPU (part numbers TSXP5*, all versions). **CVE ID : CVE-2021-22792**		
modicon_premium_tsxp57_554m					
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://download.schneider-electric.com/files?p_Doc_Ref=SEVD-2021-222-04	H-SCH-MODI-180921/2067

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 EcoStruxureª Control Expert, 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), 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	https://download.schneider-electric.com/files?p_Doc_Ref=SEVD-2021-222-04	H-SCH-MODI-180921/2068

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			(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 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). **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 EcoStruxureª Control Expert, including all Unity Pro versions (former name of EcoStruxureª Control Expert,	https://download.schneider-electric.com/files?p_Doc_Ref=SEVD-2021-222-04	H-SCH-MODI-180921/2069

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://download.schneider-electric.com/files?p_Doc_Ref=SEVD-2021-222-04	H-SCH-MODI-180921/2070

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_premium_tsxp57_5634m					
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 EcoStruxureª Control Expert, 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), Modicon	https://download.schneider-electric.com/files?p_Doc_Ref=SEVD-2021-222-04	H-SCH-MODI-180921/2071

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://download.schneider-electric.com/files?p_Doc_Ref=SEVD-2021-222-04	H-SCH-MODI-180921/2072

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 EcoStruxureª Control Expert, 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), Modicon Quantum CPU (part numbers 140CPU*, all versions), Modicon Premium CPU (part numbers TSXP5*, all versions). **CVE ID : CVE-2021-22791**	https://download.schneider-electric.com/files?p_Doc_Ref=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://download.schneider-electric.com/f	H-SCH-MODI-180921/2074

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 EcoStruxureª Control Expert, 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), Modicon Quantum CPU (part numbers 140CPU*, all versions), Modicon Premium CPU (part numbers TSXP5*, all versions). **CVE ID : CVE-2021-22792**	iles?p_Doc_Ref=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://download.schneider-electric.com/files?p_Doc_Ref=SEVD-2021-222-04	H-SCH-MODI-180921/2075

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 EcoStruxureª Control Expert, 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), 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://download.schneider-electric.com/files?p_Doc_Ref=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™ 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), 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	https://download.schneider-electric.com/files?p_Doc_Ref=SEVD-2021-222-04	H-SCH-MODI-180921/2077

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			(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 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). **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 EcoStruxureª Control Expert, including all Unity Pro versions (former name of	https://download.schneider-electric.com/files?p_Doc_Ref=SEVD-2021-222-04	H-SCH-MODI-180921/2078

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			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). **CVE ID : CVE-2021-22792**		
modicon_quantum_140cpu65150					
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 EcoStruxureª Control Expert, including all Unity Pro versions (former name of EcoStruxureª Control Expert,	https://download.schneider-electric.com/files?p_Doc_Ref=SEVD-2021-222-04	H-SCH-MODI-180921/2079

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://download.schneider-electric.com/files?p_Doc_Ref=SEVD-2021-222-04	H-SCH-MODI-180921/2080

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://download.schneider-electric.com/files?p_Doc_Ref=SEVD-2021-222-04	H-SCH-MODI-180921/2081

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 EcoStruxureª Control Expert, 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), Modicon Quantum CPU (part numbers 140CPU*, all versions), Modicon Premium CPU (part numbers TSXP5*, all versions). **CVE ID : CVE-2021-22792**	https://download.schneider-electric.com/files?p_Doc_Ref=SEVD-2021-222-04	H-SCH-MODI-180921/2082
modicon_quantum_140cpu65150c					
Improper Restriction	02-Sep-21	4	A CWE-119: Improper Restriction of Operations	https://download.schneide	H-SCH-MODI-180921/2083

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
of Operations within the Bounds of a Memory Buffer			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 EcoStruxureª Control Expert, 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), Modicon Quantum CPU (part numbers 140CPU*, all versions), Modicon Premium CPU (part numbers TSXP5*, all versions). **CVE ID : CVE-2021-22789**	r-electric.com/files?p_Doc_Ref=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://download.schneider-electric.com/files?p_Doc_Re	H-SCH-MODI-180921/2084

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 EcoStruxureª Control Expert, 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), Modicon Quantum CPU (part numbers 140CPU*, all versions), Modicon Premium CPU (part numbers TSXP5*, all versions). **CVE ID : CVE-2021-22790**	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://download.schneider-electric.com/files?p_Doc_Ref=SEVD-2021-222-04	H-SCH-MODI-180921/2085

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			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 of 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). **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	https://download.schneider-electric.com/files?p_Doc_Ref=SEVD-2021-222-04	H-SCH-MODI-180921/2086

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			(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 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). **CVE ID : CVE-2021-22792**		
modicon_quantum_140cpu65160					
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://download.schneider-electric.com/files?p_Doc_Ref=SEVD-2021-222-04	H-SCH-MODI-180921/2087

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			versions), PLC Simulator for EcoStruxureª Control Expert, 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), 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 EcoStruxureª Control Expert, including all Unity Pro versions (former name of EcoStruxureª Control Expert, all versions), PLC Simulator	https://download.schneider-electric.com/files?p_Doc_Ref=SEVD-2021-222-04	H-SCH-MODI-180921/2088

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			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, all versions), Modicon Quantum CPU (part numbers	https://download.schneider-electric.com/files?p_Doc_Ref=SEVD-2021-222-04	H-SCH-MODI-180921/2089

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			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 EcoStruxureª Control Expert, 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), Modicon Quantum CPU (part numbers 140CPU*, all versions), Modicon Premium CPU (part numbers TSXP5*, all versions).	https://download.schneider-electric.com/files?p_Doc_Ref=SEVD-2021-222-04	H-SCH-MODI-180921/2090

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2021-22792		
modicon_quantum_140cpu65160c					
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 EcoStruxureª Control Expert, 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), Modicon Quantum CPU (part numbers 140CPU*, all versions), Modicon Premium CPU (part numbers TSXP5*, all versions). **CVE ID : CVE-2021-22789**	https://download.schneider-electric.com/files?p_Doc_Ref=SEVD-2021-222-04	H-SCH-MODI-180921/2091

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 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 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). **CVE ID : CVE-2021-22790**	https://download.schneider-electric.com/files?p_Doc_Ref=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://download.schneider-electric.com/files?p_Doc_Ref=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 EcoStruxureª Control Expert, 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), Modicon Quantum CPU (part numbers 140CPU*, all versions), Modicon Premium CPU (part numbers TSXP5*, all versions). **CVE ID : CVE-2021-22791**	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://download.schneider-electric.com/files?p_Doc_Ref=SEVD-2021-222-04	H-SCH-MODI-180921/2094

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 EcoStruxureª Control Expert, 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), Modicon Quantum CPU (part numbers 140CPU*, all versions), Modicon Premium CPU (part numbers TSXP5*, all versions). **CVE ID : CVE-2021-22792**		
plc_simulator_for_ecostruxure_control_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),	https://download.schneider-electric.com/files?p_Doc_Ref=SEVD-2021-222-04	H-SCH-PLC_-180921/2095

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 EcoStruxureª Control Expert, 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), 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	https://download.schneider-electric.com/files?p_Doc_Ref=SEVD-2021-222-04	H-SCH-PLC_-180921/2096

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			EcoStruxureª Control Expert, 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), 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 EcoStruxureª Control Expert, including all Unity Pro versions (former name of EcoStruxureª Control Expert, all versions), PLC Simulator for EcoStruxureª Process	https://download.schneider-electric.com/files?p_Doc_Ref=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® 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® 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), Modicon Quantum CPU (part numbers	https://download.schneider-electric.com/files?p_Doc_Ref=SEVD-2021-222-04	H-SCH-PLC_-180921/2098

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			140CPU*, all versions), Modicon Premium CPU (part numbers TSXP5*, all versions). **CVE ID : CVE-2021-22792**		
plc_simulator_for_ecostruxure_process_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 EcoStruxureª Control Expert, 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), Modicon Quantum CPU (part numbers 140CPU*, all versions),	https://download.schneider-electric.com/files?p_Doc_Ref=SEVD-2021-222-04	H-SCH-PLC_-180921/2099

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			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 EcoStruxureª Control Expert, 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), Modicon Quantum CPU (part numbers 140CPU*, all versions), Modicon Premium CPU (part numbers TSXP5*, all versions). **CVE ID : CVE-2021-22790**	https://download.schneider-electric.com/files?p_Doc_Ref=SEVD-2021-222-04	H-SCH-PLC_-180921/2100
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 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 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), Modicon Quantum CPU (part numbers 140CPU*, all versions), Modicon Premium CPU (part numbers TSXP5*, all versions). **CVE ID : CVE-2021-22791**	load.schneider-electric.com/files?p_Doc_Ref=SEVD-2021-222-04	180921/2101
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	https://download.schneider-electric.com/files?p_Doc_Ref=SEVD-	H-SCH-PLC_-180921/2102

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 EcoStruxureª Control Expert, 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), 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/wireless/bluetooth/bluegiga-classic-legacy-modules/device.wt32i-a	H-SIL-WT32-180921/2103

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			packet. **CVE ID : CVE-2021-31609**		
ti					
cc256xcqfn-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/product/CC2564C, https://www.ti.com/tool/CC256XC-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/product/68-cn.html	H-ZH--AC69-180921/2105
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-ZH--AC69-180921/2106

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/product/68-cn.html	H-ZH--AC69-180921/2107
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/product/68-cn.html	H-ZH--AC69-180921/2108
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-ZH--AC69-180921/2109

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					
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/product/68-cn.html	H-ZH--AC69-180921/2110
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/product/68-cn.html	H-ZH--AC69-180921/2111
ac6907					
N/A	07-Sep-21	6.1	The Bluetooth Classic	http://www.	H-ZH--AC69-

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/product/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/product/68-cn.html	H-ZH--AC69-180921/2113
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/product/68-cn.html	H-ZH--AC69-180921/2114

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/product/68-cn.html	H-ZH--AC69-180921/2115
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/product/68-cn.html	H-ZH--AC69-180921/2116
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/product/68-cn.html	H-ZH--AC69-180921/2117

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. **CVE ID : CVE-2021-31613**	http://www.zh-jieli.com/product/68-cn.html	H-ZH--AC69-180921/2118
ac6926					
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/product/68-cn.html	H-ZH--AC69-180921/2119
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/product/68-	H-ZH--AC69-180921/2120

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/product/68-cn.html	H-ZH--AC69-180921/2121
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/product/68-cn.html	H-ZH--AC69-180921/2122
ac692n					

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/product/68-cn.html	H-ZH--AC69-180921/2123
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-ZH--AC69-180921/2124
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-ZH--AC69-180921/2125

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					
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-ZH--AC69-180921/2126
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-ZH--AC69-180921/2127

Weakness	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**		
ac6952					
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-ZH--AC69-180921/2128
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	N/A	H-ZH--AC69-180921/2129

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-ZH--AC69-180921/2130
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-ZH--AC69-180921/2131

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2021-34144		
ac6955					
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-ZH--AC69-180921/2132
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-ZH--AC69-180921/2133
ac6956					

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-ZH--AC69-180921/2134
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-ZH--AC69-180921/2135
ac6963					
N/A	07-Sep-21	6.1	The Bluetooth Classic implementation in the Zhuhai Jieli AC6366C_DEMO_V1.0	N/A	H-ZH--AC69-180921/2136

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			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-ZH--AC69-180921/2137
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-ZH--AC69-180921/2138

Weakness	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**		
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-ZH--AC69-180921/2139
ac6966					
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	N/A	H-ZH--AC69-180921/2140

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-ZH--AC69-180921/2141
ac6969					
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	N/A	H-ZH--AC69-180921/2142

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			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-ZH--AC69-180921/2143
ac6973					
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-ZH--AC69-180921/2144

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 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-ZH--AC69-180921/2145
ac6976					
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-ZH--AC69-180921/2146
N/A	07-Sep-21	3.3	The Bluetooth Classic	N/A	H-ZH--AC69-

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			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**		180921/2147
ac6983					
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-ZH--AC69-180921/2148
N/A	07-Sep-21	3.3	The Bluetooth Classic implementation in the Zhuhai Jieli AC6366C BT SDK through 0.9.1 does not	N/A	H-ZH--AC69-180921/2149

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					
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-ZH--AC69-180921/2150
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-ZH--AC69-180921/2151

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			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**		
ac6997					
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/product/68-cn.html	H-ZH--AC69-180921/2152
ac6998					
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/product/68-cn.html	H-ZH--AC69-180921/2153

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2021-31612		
ac6999					
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/product/68-cn.html	H-ZH--AC69-180921/2154
Operating System					
actions-semi					
ats2815_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 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/index.php?id=3581&siteId=4	O-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/index.php?id=35	O-ACT-ATS2-200921/2156

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_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 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/index.php?id=3581&siteId=4	O-ACT-ATS2-200921/2157
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	https://www.actions-semi.com/index.php?id=3581&siteId=4	O-ACT-ATS2-200921/2158

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			with a forged BDAddress that matches the original connected host. **CVE ID : CVE-2021-31786**		
ats2819s_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 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/index.php?id=3581&siteId=4	O-ACT-ATS2-200921/2159
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/index.php?id=3581&siteId=4	O-ACT-ATS2-200921/2160
ats2819t_firmware					

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/index.php?id=3581&siteId=4	O-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/index.php?id=3581&siteId=4	O-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/index.php?id=3581&siteId=4	O-ACT-ATS2-200921/2163

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/index.php?id=3581&siteId=4	O-ACT-ATS2-200921/2164
Amazon					
kindle_firmware					
Integer Overflow or Wraparound	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

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Improper Privilege Management	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	O-AMA-KIND-200921/2166
Apple					
ipados					
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://support.apple.com/en-us/HT212604, https://support.apple.com/en-us/HT212605, https://support.apple.com/en-us/HT212602, https://support.apple.com/en-us/HT212603, https://support.apple.com/en-us/HT212600, https://support.apple.com/en-us/HT212601	O-APP-IPAD-200921/2167

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://support.apple.com/en-us/HT212605, https://support.apple.com/en-us/HT212601	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://support.apple.com/en-us/HT212317, https://support.apple.com/en-us/HT212323, https://support.apple.com/en-us/HT212324	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://support.apple.com/en-us/HT212606, https://support.apple.com/en-us/HT212604, https://support.apple.com/en-us/HT212605,	O-APP-IPAD-200921/2170

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
				https://support.apple.com/en-us/HT212602, https://support.apple.com/en-us/HT212601	
ipad_os					
Improper Authentication	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://support.apple.com/en-us/HT212529, https://support.apple.com/en-us/HT212528, https://support.apple.com/en-us/HT212534, https://support.apple.com/en-us/HT212532, https://support.apple.com/en-us/HT212533	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://support.apple.com/en-	O-APP-IPAD-200921/2172

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/HT212530, https://support.apple.com/en-us/HT212531, https://support.apple.com/en-us/HT212529, https://support.apple.com/en-us/HT212528, https://support.apple.com/en-us/HT212532, https://support.apple.com/en-us/HT212533	
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://support.apple.com/en-us/HT212529, https://support.apple.com/en-us/HT212528, https://support.apple.com/en-	O-APP-IPAD-200921/2173

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
				us/HT212532, https://support.apple.com/en-us/HT212533	
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://support.apple.com/en-us/HT212528	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://support.apple.com/en-us/HT212529, https://support.apple.com/en-us/HT212528, https://support.apple.com/en-us/HT212603, https://support.apple.com/en-us/HT212600, https://support.apple.com/en-us/HT212532,	O-APP-IPAD-200921/2175

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
				https://support.apple.com/en-us/HT212533	
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://support.apple.com/en-us/HT212529, https://support.apple.com/en-us/HT212528, https://support.apple.com/en-us/HT212534, https://support.apple.com/en-us/HT212532, https://support.apple.com/en-us/HT212533	O-APP-IPAD-200921/2176
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.	https://support.apple.com/en-us/HT212529, https://support.apple.com/en-us/HT212528,	O-APP-IPAD-200921/2177

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2021-30736	https://support.apple.com/en-us/HT212532, https://support.apple.com/en-us/HT212533	
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://support.apple.com/en-us/HT212530, https://support.apple.com/en-us/HT212531, https://support.apple.com/en-us/HT212529, https://support.apple.com/en-us/HT212528, https://support.apple.com/en-us/HT212548, https://support.apple.com/en-us/HT212532	O-APP-IPAD-200921/2178

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
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://support.apple.com/en-us/HT212529, https://support.apple.com/en-us/HT212528, https://support.apple.com/en-us/HT212532, https://support.apple.com/en-us/HT212533	O-APP-IPAD-200921/2179
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://support.apple.com/en-us/HT212528	O-APP-IPAD-200921/2180
Uncontrolled Resource Consumption	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.	https://support.apple.com/en-us/HT212317	O-APP-IPAD-200921/2181

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://support.apple.com/en-us/HT212530, https://support.apple.com/en-us/HT212317, https://support.apple.com/en-us/HT212325, https://support.apple.com/en-us/HT212323, https://support.apple.com/en-us/HT212324	O-APP-IPAD-200921/2182
iphone_os					
N/A	02-Sep-21	4	Microsoft Edge for iOS Spoofing Vulnerability **CVE ID : CVE-2021-38642**	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2021-38642	O-APP-IPHO-200921/2183
Improper Authentication	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://support.apple.com/en-us/HT212529,	O-APP-IPHO-200921/2184

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. **CVE ID : CVE-2021-30720**	https://support.apple.com/en-us/HT212528, https://support.apple.com/en-us/HT212534, https://support.apple.com/en-us/HT212532, https://support.apple.com/en-us/HT212533	
Improper Privilege Management	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://support.apple.com/en-us/HT212530, https://support.apple.com/en-us/HT212531, https://support.apple.com/en-us/HT212529, https://support.apple.com/en-us/HT212528,	O-APP-IPHO-200921/2185

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
				https://support.apple.com/en-us/HT212532, https://support.apple.com/en-us/HT212533	
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://support.apple.com/en-us/HT212529, https://support.apple.com/en-us/HT212528, https://support.apple.com/en-us/HT212532, https://support.apple.com/en-us/HT212533	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://support.apple.com/en-us/HT212528	O-APP-IPHO-200921/2187
Out-of-bounds	08-Sep-21	4.3	An out-of-bounds read was addressed with improved	https://support.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/HT212529, https://support.apple.com/en-us/HT212528, https://support.apple.com/en-us/HT212603, https://support.apple.com/en-us/HT212600, https://support.apple.com/en-us/HT212532, https://support.apple.com/en-us/HT212533	
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://support.apple.com/en-us/HT212529, https://support.apple.com/en-us/HT212528, https://support.apple.com	O-APP-IPHO-200921/2189

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
				/en-us/HT212534, https://support.apple.com/en-us/HT212532, https://support.apple.com/en-us/HT212533	
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://support.apple.com/en-us/HT212529, https://support.apple.com/en-us/HT212528, https://support.apple.com/en-us/HT212532, https://support.apple.com/en-us/HT212533	O-APP-IPHO-200921/2190
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	https://support.apple.com/en-us/HT212530, https://support.apple.com	O-APP-IPHO-200921/2191

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			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**	/en-us/HT212531, https://support.apple.com/en-us/HT212529, https://support.apple.com/en-us/HT212528, https://support.apple.com/en-us/HT212548, https://support.apple.com/en-us/HT212532	
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://support.apple.com/en-us/HT212529, https://support.apple.com/en-us/HT212528, https://support.apple.com/en-us/HT212532, https://support.apple.com	O-APP-IPHO-200921/2192

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
				/en-us/HT212533	
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://support.apple.com/en-us/HT212528	O-APP-IPHO-200921/2193
Uncontrolled Resource Consumption	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://support.apple.com/en-us/HT212317	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://support.apple.com/en-us/HT212530, https://support.apple.com/en-us/HT212317, https://support.apple.com/en-us/HT212325, https://supp	O-APP-IPHO-200921/2195

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
				ort.apple.com/en-us/HT212323, https://support.apple.com/en-us/HT212324	
Access of Resource Using Incompatible 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://support.apple.com/en-us/HT212606, https://support.apple.com/en-us/HT212604, https://support.apple.com/en-us/HT212605, https://support.apple.com/en-us/HT212602, https://support.apple.com/en-us/HT212601	O-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://support.apple.com/en-us/HT212604, https://supp	O-APP-IPHO-200921/2197

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/HT212605, https://support.apple.com/en-us/HT212602, https://support.apple.com/en-us/HT212603, https://support.apple.com/en-us/HT212600, https://support.apple.com/en-us/HT212601	
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://support.apple.com/en-us/HT212548	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://support.apple.com/en-	O-APP-IPHO-200921/2199

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			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/HT212548	
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://support.apple.com/en-us/HT212605, https://support.apple.com/en-us/HT212601	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://support.apple.com/en-us/HT212317, https://support.apple.com/en-us/HT212323, https://support.apple.com/en-us/HT212324	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://support.apple.com/en-us/HT212606, https://supp	O-APP-IPHO-200921/2202

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			crafted web content may lead to code execution. **CVE ID : CVE-2021-30797**	ort.apple.com/en-us/HT212604, https://support.apple.com/en-us/HT212605, https://support.apple.com/en-us/HT212602, https://support.apple.com/en-us/HT212601	
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://support.apple.com/en-us/HT212605, https://support.apple.com/en-us/HT212602, https://support.apple.com/en-us/HT212601	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/security/products/acrobat/	O-APP-MACO-200921/2204

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/security/products/integrity_service/apsb21-27.html	O-APP-MACO-200921/2205
Access of Resource Using Incompatible 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://support.apple.com/en-us/HT212606, https://support.apple.com/en-us/HT212604, https://support.apple.com/en-us/HT21260	O-APP-MACO-200921/2206

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
				5, https://support.apple.com/en-us/HT212602, https://support.apple.com/en-us/HT212601	
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://support.apple.com/en-us/HT212604, https://support.apple.com/en-us/HT212605, https://support.apple.com/en-us/HT212602, https://support.apple.com/en-us/HT212603, https://support.apple.com/en-us/HT212600, https://support.apple.com/en-us/HT21260	O-APP-MACO-200921/2207

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://support.apple.com/en-us/HT212606, https://support.apple.com/en-us/HT212604, https://support.apple.com/en-us/HT212605, https://support.apple.com/en-us/HT212602, https://support.apple.com/en-us/HT212601	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://support.apple.com/en-us/HT212605, https://support.apple.com/en-us/HT212602, https://support.apple.com/en-us/HT21260	O-APP-MACO-200921/2209

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
				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/en/business/programs/vulnerability-reward-program/hall-of-fame, https://www.f-secure.com/en/business/support-and-downloads/security-advisories/cve-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/security/products/photoshop/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/security/products/photoshop/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 Authentication	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://support.apple.com/en-us/HT212529, https://support.apple.com/en-us/HT212528, https://support.apple.com/en-us/HT212534, https://support.apple.com/en-us/HT212532, https://support.apple.com/en-us/HT212533	O-APP-MAC_-200921/2213
Improper Privilege Management	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://support.apple.com/en-us/HT212530, https://support.apple.com	O-APP-MAC_-200921/2214

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			11.4, watchOS 7.5. A local attacker may be able to elevate their privileges. **CVE ID : CVE-2021-30724**	/en-us/HT212531, https://support.apple.com/en-us/HT212529, https://support.apple.com/en-us/HT212528, https://support.apple.com/en-us/HT212532, https://support.apple.com/en-us/HT212533	
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://support.apple.com/en-us/HT212529, https://support.apple.com/en-us/HT212528, https://support.apple.com/en-us/HT212532, https://support.apple.com	O-APP-MAC_-200921/2215

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
				/en-us/HT212533	
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://support.apple.com/en-us/HT212529, https://support.apple.com/en-us/HT212528, https://support.apple.com/en-us/HT212603, https://support.apple.com/en-us/HT212600, https://support.apple.com/en-us/HT212532, https://support.apple.com/en-us/HT212533	O-APP-MAC_-200921/2216
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.	https://support.apple.com/en-us/HT212529, https://support.apple.com	O-APP-MAC_-200921/2217

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/HT212528, https://support.apple.com/en-us/HT212534, https://support.apple.com/en-us/HT212532, https://support.apple.com/en-us/HT212533	
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://support.apple.com/en-us/HT212530, https://support.apple.com/en-us/HT212531, https://support.apple.com/en-us/HT212529	O-APP-MAC_-200921/2218
Buffer Copy without Checking Size of Input ('Classic Buffer	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	https://support.apple.com/en-us/HT212529, https://support.apple.com	O-APP-MAC_-200921/2219

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Overflow')			execute arbitrary code with kernel privileges. **CVE ID : CVE-2021-30736**	/en-us/HT212528, https://support.apple.com/en-us/HT212532, https://support.apple.com/en-us/HT212533	
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://support.apple.com/en-us/HT212530, https://support.apple.com/en-us/HT212531, https://support.apple.com/en-us/HT212529, https://support.apple.com/en-us/HT212528, https://support.apple.com/en-us/HT212548, https://support.apple.com	O-APP-MAC_-200921/2220

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
				/en-us/HT212532	
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://support.apple.com/en-us/HT212531, https://support.apple.com/en-us/HT212529	O-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://support.apple.com/en-us/HT212530, https://support.apple.com/en-us/HT212531, https://support.apple.com/en-us/HT212529	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://support.apple.com/en-us/HT212529, https://support.apple.com/en-us/HT212528, https://supp	O-APP-MAC_-200921/2223

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
				ort.apple.com/en-us/HT212532, https://support.apple.com/en-us/HT212533	
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://support.apple.com/en-us/HT212530, https://support.apple.com/en-us/HT212317, https://support.apple.com/en-us/HT212325, https://support.apple.com/en-us/HT212323, https://support.apple.com/en-us/HT212324	O-APP-MAC_-200921/2224
mac_os_x					
Improper Privilege Management	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://support.apple.com/en-us/HT21253	O-APP-MAC_-200921/2225

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://support.apple.com/en-us/HT212531, https://support.apple.com/en-us/HT212529, https://support.apple.com/en-us/HT212528, https://support.apple.com/en-us/HT212532, https://support.apple.com/en-us/HT212533	
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://support.apple.com/en-us/HT212529, https://support.apple.com/en-us/HT212528, https://support.apple.com/en-us/HT21260	O-APP-MAC_-200921/2226

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
				3, https://support.apple.com/en-us/HT212600, https://support.apple.com/en-us/HT212532, https://support.apple.com/en-us/HT212533	
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://support.apple.com/en-us/HT212530, https://support.apple.com/en-us/HT212531, https://support.apple.com/en-us/HT212529	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://support.apple.com/en-us/HT212530, https://support.apple.com/en-us/HT212533	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://support.apple.com/en-us/HT212529, https://support.apple.com/en-us/HT212528, https://support.apple.com/en-us/HT212548, https://support.apple.com/en-us/HT212532	
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://support.apple.com/en-us/HT212531, https://support.apple.com/en-us/HT212529	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://support.apple.com/en-us/HT212530, https://support.apple.com/en-	O-APP-MAC_-200921/2230

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			improved validation. **CVE ID : CVE-2021-30739**	us/HT212531, https://support.apple.com/en-us/HT212529	
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://support.apple.com/en-us/HT212530, https://support.apple.com/en-us/HT212317, https://support.apple.com/en-us/HT212325, https://support.apple.com/en-us/HT212323, https://support.apple.com/en-us/HT212324	O-APP-MAC_-200921/2231
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.	https://support.apple.com/en-us/HT212604, https://support.apple.com/en-	O-APP-MAC_-200921/2232

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/HT212605, https://support.apple.com/en-us/HT212602, https://support.apple.com/en-us/HT212603, https://support.apple.com/en-us/HT212600, https://support.apple.com/en-us/HT212601	
tvos					
Improper Authentication	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://support.apple.com/en-us/HT212529, https://support.apple.com/en-us/HT212528, https://support.apple.com/en-us/HT212534, https://support.apple.com	O-APP-TVOS-200921/2233

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
				/en-us/HT212532, https://support.apple.com/en-us/HT212533	
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://support.apple.com/en-us/HT212529, https://support.apple.com/en-us/HT212528, https://support.apple.com/en-us/HT212532, https://support.apple.com/en-us/HT212533	O-APP-TVOS-200921/2234
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	https://support.apple.com/en-us/HT212529, https://support.apple.com/en-us/HT212528, https://support.apple.com	O-APP-TVOS-200921/2235

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			process memory. **CVE ID : CVE-2021-30733**	/en-us/HT212603, https://support.apple.com/en-us/HT212600, https://support.apple.com/en-us/HT212532, https://support.apple.com/en-us/HT212533	
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://support.apple.com/en-us/HT212529, https://support.apple.com/en-us/HT212528, https://support.apple.com/en-us/HT212534, https://support.apple.com/en-us/HT212532, https://support.apple.com	O-APP-TVOS-200921/2236

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
				/en-us/HT212533	
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://support.apple.com/en-us/HT212529, https://support.apple.com/en-us/HT212528, https://support.apple.com/en-us/HT212532, https://support.apple.com/en-us/HT212533	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://support.apple.com/en-us/HT212530, https://support.apple.com/en-us/HT212531, https://support.apple.com/en-us/HT212529, https://support.apple.com	O-APP-TVOS-200921/2238

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
				/en-us/HT212528, https://support.apple.com/en-us/HT212548, https://support.apple.com/en-us/HT212532	
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://support.apple.com/en-us/HT212529, https://support.apple.com/en-us/HT212528, https://support.apple.com/en-us/HT212532, https://support.apple.com/en-us/HT212533	O-APP-TVOS-200921/2239
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	https://support.apple.com/en-us/HT212530, https://support.apple.com	O-APP-TVOS-200921/2240

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			11.3. Processing a maliciously crafted image may lead to arbitrary code execution. **CVE ID : CVE-2021-30743**	/en-us/HT212317, https://support.apple.com/en-us/HT212325, https://support.apple.com/en-us/HT212323, https://support.apple.com/en-us/HT212324	
Access of Resource Using Incompatible 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://support.apple.com/en-us/HT212606, https://support.apple.com/en-us/HT212604, https://support.apple.com/en-us/HT212605, https://support.apple.com/en-us/HT212602, https://support.apple.com	O-APP-TVOS-200921/2241

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
				/en-us/HT212601	
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://support.apple.com/en-us/HT212604, https://support.apple.com/en-us/HT212605, https://support.apple.com/en-us/HT212602, https://support.apple.com/en-us/HT212603, https://support.apple.com/en-us/HT212600, https://support.apple.com/en-us/HT212601	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://support.apple.com/en-us/HT212317, https://support.apple.com	O-APP-TVOS-200921/2243

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			checks. **CVE ID : CVE-2021-30764**	/en-us/HT212323, https://support.apple.com/en-us/HT212324	
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://support.apple.com/en-us/HT212606, https://support.apple.com/en-us/HT212604, https://support.apple.com/en-us/HT212605, https://support.apple.com/en-us/HT212602, https://support.apple.com/en-us/HT212601	O-APP-TVOS-200921/2244
watchos					
Improper Authentication	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://support.apple.com/en-us/HT212529,	O-APP-WATC-200921/2245

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. **CVE ID : CVE-2021-30720**	https://support.apple.com/en-us/HT212528, https://support.apple.com/en-us/HT212534, https://support.apple.com/en-us/HT212532, https://support.apple.com/en-us/HT212533	
Improper Privilege Management	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://support.apple.com/en-us/HT212530, https://support.apple.com/en-us/HT212531, https://support.apple.com/en-us/HT212529, https://support.apple.com/en-us/HT212528,	O-APP-WATC-200921/2246

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
				https://support.apple.com/en-us/HT212532, https://support.apple.com/en-us/HT212533	
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://support.apple.com/en-us/HT212529, https://support.apple.com/en-us/HT212528, https://support.apple.com/en-us/HT212532, https://support.apple.com/en-us/HT212533	O-APP-WATC-200921/2247
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	https://support.apple.com/en-us/HT212529, https://support.apple.com/en-us/HT212528,	O-APP-WATC-200921/2248

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			result in the disclosure of process memory. **CVE ID : CVE-2021-30733**	https://support.apple.com/en-us/HT212603, https://support.apple.com/en-us/HT212600, https://support.apple.com/en-us/HT212532, https://support.apple.com/en-us/HT212533	
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://support.apple.com/en-us/HT212529, https://support.apple.com/en-us/HT212528, https://support.apple.com/en-us/HT212534, https://support.apple.com/en-us/HT212532,	O-APP-WATC-200921/2249

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
				https://support.apple.com/en-us/HT212533	
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://support.apple.com/en-us/HT212529, https://support.apple.com/en-us/HT212528, https://support.apple.com/en-us/HT212532, https://support.apple.com/en-us/HT212533	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://support.apple.com/en-us/HT212530, https://support.apple.com/en-us/HT212531, https://support.apple.com/en-us/HT212529,	O-APP-WATC-200921/2251

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
				https://support.apple.com/en-us/HT212528, https://support.apple.com/en-us/HT212548, https://support.apple.com/en-us/HT212532	
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://support.apple.com/en-us/HT212529, https://support.apple.com/en-us/HT212528, https://support.apple.com/en-us/HT212532, https://support.apple.com/en-us/HT212533	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://support.apple.com/en-us/HT212530,	O-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://support.apple.com/en-us/HT212317, https://support.apple.com/en-us/HT212325, https://support.apple.com/en-us/HT212323, https://support.apple.com/en-us/HT212324	
Access of Resource Using Incompatible 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://support.apple.com/en-us/HT212606, https://support.apple.com/en-us/HT212604, https://support.apple.com/en-us/HT212605, https://support.apple.com/en-us/HT212602,	O-APP-WATC-200921/2254

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
				https://support.apple.com/en-us/HT212601	
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://support.apple.com/en-us/HT212604, https://support.apple.com/en-us/HT212605, https://support.apple.com/en-us/HT212602, https://support.apple.com/en-us/HT212603, https://support.apple.com/en-us/HT212600, https://support.apple.com/en-us/HT212601	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://support.apple.com/en-us/HT212605,	O-APP-WATC-200921/2256

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			bypass Internet permission requirements. **CVE ID : CVE-2021-30763**	https://support.apple.com/en-us/HT212601	
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://support.apple.com/en-us/HT212317, https://support.apple.com/en-us/HT212323, https://support.apple.com/en-us/HT212324	O-APP-WATC-200921/2257
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://support.apple.com/en-us/HT212606, https://support.apple.com/en-us/HT212604, https://support.apple.com/en-us/HT212605, https://support.apple.com/en-us/HT212602,	O-APP-WATC-200921/2258

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
				https://support.apple.com/en-us/HT212601	
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://support.apple.com/en-us/HT212605, https://support.apple.com/en-us/HT212602, https://support.apple.com/en-us/HT212601	O-APP-WATC-200921/2259
Arubanetworks					
arubaos					
Improper Neutralization 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-2021-37722**	https://www.arubanetworks.com/assets/alert/ARUBA-PSA-2021-016.txt	O-ARU-ARUB-200921/2260
Improper	07-Sep-21	9	A remote arbitrary command	https://www.	O-ARU-ARUB-

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Neutralization 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**	arubanetworks.com/assets/alert/ARUBA-PSA-2021-016.txt	200921/2261
Improper Neutralization 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.arubanetworks.com/assets/alert/ARUBA-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.arubanetworks.com/assets/alert/ARUBA-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.arubanetworks.com/assets/alert/ARUB	O-ARU-ARUB-200921/2264

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.arubanetworks.com/assets/alert/ARUBA-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.arubanetworks.com/assets/alert/ARUBA-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.arubanetworks.com/asset	O-ARU-ARUB-200921/2267

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Pathname to a Restricted Directory ('Path Traversal')			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**	s/alert/ARUBA-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.arubanetworks.com/assets/alert/ARUBA-PSA-2021-016.txt	O-ARU-ARUB-200921/2268
Improper Neutralization 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.arubanetworks.com/assets/alert/ARUBA-PSA-2021-016.txt	O-ARU-ARUB-200921/2269

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2021-37717		
Improper Neutralization 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.arubanetworks.com/assets/alert/ARUBA-PSA-2021-016.txt	O-ARU-ARUB-200921/2270
Improper Neutralization 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.arubanetworks.com/assets/alert/ARUBA-PSA-2021-016.txt	O-ARU-ARUB-200921/2271
Improper Neutralization 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.	https://www.arubanetworks.com/assets/alert/ARUBA-PSA-2021-016.txt	O-ARU-ARUB-200921/2272

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 Neutralization 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.arubanetworks.com/assets/alert/ARUBA-PSA-2021-016.txt	O-ARU-ARUB-200921/2273
sd-wan					
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.arubanetworks.com/assets/alert/ARUBA-PSA-2021-016.txt	O-ARU-SD-W-200921/2274
Improper	07-Sep-21	7.2	A local path traversal	https://www.	O-ARU-SD-W-

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**	arubanetworks.com/assets/alert/ARUBA-PSA-2021-016.txt	200921/2275
Improper Limitation of a Pathname to a Restricted Directory ('Path Traversal')	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.arubanetworks.com/assets/alert/ARUBA-PSA-2021-016.txt	O-ARU-SD-W-200921/2276
bluetrum					
ab5301a_firmware					
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	http://www.bluetrum.com/product/ab5301a.html	O-BLU-AB53-200921/2277

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. **CVE ID : CVE-2021-34150**		
ab5376t_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 device) by flooding a device with LMP_AU_rand data. **CVE ID : CVE-2021-31610**	http://www.bluetrum.com/product/ab5376t.html, http://www.bluetrum.com/product/bt8896a.html	O-BLU-AB53-200921/2278
bt8896a_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 device) by flooding a device with LMP_AU_rand data. **CVE ID : CVE-2021-31610**	http://www.bluetrum.com/product/ab5376t.html, http://www.bluetrum.com/product/bt8896a.html	O-BLU-BT88-200921/2279
christiedigital					

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
dwu850-gs_firmware					
Improper Authentication	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_firmware					
Missing Authorization	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 Management	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 Authentication	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

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2021-40380		
Improper Privilege Management	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-IP57-200921/2284
Improper Privilege Management	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-IP57-200921/2285
ip60_firmware					
Missing Authorization	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-IP60-200921/2286
Improper Privilege Management	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 Authentication	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	O-COM-IP60-200921/2288

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			credentials. **CVE ID : CVE-2021-40380**		
Improper Privilege Management	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 Management	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_firmware					
Missing Authorization	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 Management	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 Authentication	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

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			setcamera.cgi disclose credentials. **CVE ID : CVE-2021-40380**		
Improper Privilege Management	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
Improper Privilege Management	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-IP70-200921/2295
tn540_firmware					
Missing Authorization	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-TN54-200921/2296
Improper Privilege Management	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-TN54-200921/2297
Improper Authentication	01-Sep-21	5	An issue was discovered on Compro IP70 2.08_7130218, IP570 2.08_7130520, IP60, and TN540 devices.	N/A	O-COM-TN54-200921/2298

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			cameralist.cgi and setcamera.cgi disclose credentials. **CVE ID : CVE-2021-40380**		
Improper Privilege Management	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 Management	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://github.com/contiki-os/contiki/issues/2686	O-CON-CONT-200921/2301

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/documentation/datasheets/cyw20735b1-single-chip-bluetooth-transceiver-wireless-input-devices	O-CYP-CYW2-200921/2302
cyw920735q60evb-01_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/documentation/datasheets/cyw20735b1-single-chip-bluetooth-transceiver-wireless-input-devices	O-CYP-CYW9-200921/2303
wireless_internet_connectivity_for_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/documentation/datasheets/cyw20735b	O-CYP-WIRE-200921/2304

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 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**	1-single-chip-bluetooth-transceiver-wireless-input-devices	
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 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**	https://www.cypress.com/documentation/datasheets/cyw20735b1-single-chip-bluetooth-transceiver-wireless-input-devices	O-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/documentation/datasheets/cyw20735b1-single-chip-bluetooth-	O-CYP-WIRE-200921/2306

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. **CVE ID : CVE-2021-34148**	transceiver-wireless-input-devices	
Debian					
debian_linux					
Integer Overflow or Wraparound	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.haproxy.org/?p=haproxy.git, https://github.com/haproxy/haproxy/commit/3b69886f7dcc3cfb3d166309018e6cfec9ce2c95	O-DEB-DEBI-200921/2307
Fedoraproject					
fedora					
Out-of-bounds Write	06-Sep-21	4.6	vim is vulnerable to Heap-based Buffer Overflow **CVE ID : CVE-2021-3770**	https://github.com/vim/vim/commit/b7081e135a16091c93f6f5f7525a5c58fb7ca9f9, https://huntr.dev/bounties/016ad2f2-07c1-4d14-a8ce-6eed10729365	O-FED-FEDO-200921/2308

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Google					
android					
N/A	02-Sep-21	4	Microsoft Edge for Android Spoofing Vulnerability **CVE ID : CVE-2021-38641**	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2021-38641	O-GOO-ANDR-200921/2309
N/A	02-Sep-21	4.3	Microsoft Edge for Android Information Disclosure Vulnerability **CVE ID : CVE-2021-26439**	https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/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://chromereleases.googleblog.com/2021/08/stable-channel-update-for-desktop_31.html	O-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://chromereleases.googleblog.com/2021/08/stable-channel-update-for-desktop_31.html	O-GOO-CHRO-200921/2312

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
jbl					
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/over-ear-headphones/JBL+TUNE500BT.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/producten/experia-wifi/2	O-KPN-EXPE-200921/2314
Linux					
linux_kernel					
Concurrent Execution using	03-Sep-21	4.4	A race condition was discovered in ext4_write_inline_data_end in	https://git.kernel.org/pub/scm/linux/k	O-LIN-LINU-200921/2315

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Shared Resource with Improper Synchronization ('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/tytso/ext4.git/commit/?id=9e445093e523f3277081314c864f708fd4bd34aa	
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://chromereleases.googleblog.com/2021/08/stable-channel-update-for-desktop_31.html	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://chromereleases.googleblog.com/2021/08/stable-channel-update-for-desktop_31.html	O-LIN-LINU-200921/2317
mi					
mi_true_wireless_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	http://www.bluetrum.com/product/ab5376t.html, http://www.bluetrum.com/product/bt8896a.html	O-MI-MI_T-200921/2318

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/security/products/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/security/products/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/security/products/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/security/products/illustrator/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/security/products/illustrator/apsb21-24.html	O-MIC-WIND-200921/2323

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/security/products/illustrator/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/security/products/integrity_service/apsb21-27.html	O-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/security/products/media-encoder/apsb21-32.html	O-MIC-WIND-200921/2326

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			must open a malicious file. **CVE ID : CVE-2021-28569**		
Improper Neutralization 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/ee/security/products/after_effects/apsb21-33.html	O-MIC-WIND-200921/2327
Uncontrolled 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/security/products/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/en/business/programs/vulnerability-reward-program/hall	O-MIC-WIND-200921/2329

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/en/business/support-and-downloads/security-advisories/cve-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/security/products/after_effects/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/security/products/after_effects/apsb21-54.html	O-MIC-WIND-200921/2331

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/security/products/after_effects/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/security/products/after_effects/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/security/prod	O-MIC-WIND-200921/2334

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_effects/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/security/products/after_effects/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/security/products/bridge/apsb21-69.html	O-MIC-WIND-200921/2336

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/security/products/photoshop/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/security/products/photoshop/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/security/products/bridge/apsb21-69.html	O-MIC-WIND-200921/2339

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/security/products/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/security/products/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/security/products/media-encoder/apsb21-70.html	O-MIC-WIND-200921/2342
Out-of-	01-Sep-21	4.3	Adobe Bridge versions 11.1	https://helpx	O-MIC-WIND-

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/security/products/bridge/apsb21-69.html	200921/2343
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/security/products/bridge/apsb21-69.html	O-MIC-WIND-200921/2344
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/security/products/bridge/apsb21-69.html	O-MIC-WIND-200921/2345
Out-of-bounds	01-Sep-21	4.3	Adobe Bridge versions 11.1 (and earlier) are affected by	https://helpx.adobe.com/s	O-MIC-WIND-200921/2346

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/products/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/security/products/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/security/products/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/security/prod	O-MIC-WIND-200921/2349

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	
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/security/products/bridge/apsb21-69.html	O-MIC-WIND-200921/2350
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/security/products/bridge/apsb21-69.html	O-MIC-WIND-200921/2351
Improper Privilege	06-Sep-21	4.6	Trend Micro Security (Consumer) 2021 and 2020	https://helpcenter.trendmi	O-MIC-WIND-200921/2352

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Management			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**	cro.com/en-us/article/tmka-10568	
Moxa					
oncell_g3470a-lte-eu-t_firmware					
Improper Neutralization 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-ONCE-200921/2353
Improper Neutralization 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-ONCE-200921/2354

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2021-39279		
oncell_g3470a-lte-eu_firmware					
Improper Neutralization 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-ONCE-200921/2355
Improper Neutralization 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-ct-t_firmware					
Improper Neutralization 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

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 Neutralization 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-TAP--200921/2358
tap-323-jp-ct-t_firmware					
Improper Neutralization 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	O-MOX-TAP--200921/2359

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			3124A-US-T 2.3. **CVE ID : CVE-2021-39278**		
Improper Neutralization 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-TAP--200921/2360
tap-323-us-ct-t_firmware					
Improper Neutralization 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-TAP--200921/2361
Improper Neutralization 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

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
OS Command ('OS Command Injection')			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**		
wac-1001-t_firmware					
Improper Neutralization 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-WAC--200921/2363
Improper Neutralization 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	https://www.moxa.com	O-MOX-WAC--200921/2364

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			2.3, and WDR-3124A-US-T 2.3. **CVE ID : CVE-2021-39279**		
wac-1001_firmware					
Improper Neutralization 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-WAC--200921/2365
Improper Neutralization 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-WAC--200921/2366
wac-2004_firmware					
Improper Neutralization of Input	07-Sep-21	4.3	Certain MOXA devices allow reflected XSS via the Config Import menu. This affects	N/A	O-MOX-WAC--200921/2367

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 Neutralization 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-WAC--200921/2368
wdr-3124a-eu-t_firmware					
Improper Neutralization 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	O-MOX-WDR--200921/2369

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 Neutralization 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--200921/2370
wdr-3124a-eu_firmware					
Improper Neutralization 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 Neutralization of Special Elements	07-Sep-21	9	Certain MOXA devices allow Authenticated Command Injection via /forms/web_importTFTP.	https://www.moxa.com	O-MOX-WDR--200921/2372

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
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-us-t_firmware					
Improper Neutralization 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 Neutralization 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

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. **CVE ID : CVE-2021-39279**		
wdr-3124a-us_firmware					
Improper Neutralization 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 Neutralization 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					

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	08-Sep-21	3.5	A reflected cross-site 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. **CVE ID : CVE-2021-3052**	https://security.paloaltonetworks.com/CVE-2021-3052	O-PAL-PAN--200921/2377
Time-of-check Time-of-use (TOCTOU) Race Condition	08-Sep-21	8.5	A time-of-check to time-of-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 versions earlier than PAN-OS	https://security.paloaltonetworks.com/CVE-2021-3054	O-PAL-PAN--200921/2378

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					
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 Voice & Music, Snapdragon Wearables **CVE ID : CVE-2021-1904**	https://www.qualcomm.com/company/product-security/bulletins/august-2021-bulletin	O-QUA-APQ8-200921/2379
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.com/company/product-security/bulletins/august-2021-bulletin	O-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.com/company/product-	O-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 **CVE ID : CVE-2021-1916**	security/bulletins/august-2021-bulletin	
Integer Underflow (Wrap or Wraparound)	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.com/company/product-security/bulletins/august-2021-bulletin	O-QUA-APQ8-200921/2382
Integer Underflow (Wrap or Wraparound)	08-Sep-21	10	Integer underflow can occur due to improper 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.com/company/product-security/bulletins/august-2021-bulletin	O-QUA-APQ8-200921/2383
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.com/company/product-security/bull	O-QUA-APQ8-200921/2384

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	
apq8009_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.com/company/product-security/bulletins/august-2021-bulletin	O-QUA-APQ8-200921/2385
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.com/company/product-security/bulletins/august-2021-bulletin	O-QUA-APQ8-200921/2386

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.com/company/product-security/bulletins/august-2021-bulletin	O-QUA-APQ8-200921/2387
Integer Underflow (Wrap or Wraparound)	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.com/company/product-security/bulletins/august-2021-bulletin	O-QUA-APQ8-200921/2388
Integer Underflow (Wrap or Wraparound)	08-Sep-21	10	Integer underflow can occur due to improper 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.com/company/product-security/bulletins/august-2021-bulletin	O-QUA-APQ8-200921/2389
Out-of-	08-Sep-21	3.6	Buffer over read could occur	https://www.	O-QUA-APQ8-

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 **CVE ID : CVE-2021-1928**	qualcomm.com/company/product-security/bulletins/august-2021-bulletin	200921/2390
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	08-Sep-21	10	Possible buffer overflow due to 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 Networking **CVE ID : CVE-2021-1972**	https://www.qualcomm.com/company/product-security/bulletins/august-2021-bulletin	O-QUA-APQ8-200921/2391
apq8017_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,	https://www.qualcomm.com/company/product-security/bulletins/august-2021-bulletin	O-QUA-APQ8-200921/2392

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.com/company/product-security/bulletins/august-2021-bulletin	O-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.com/company/product-security/bulletins/august-2021-bulletin	O-QUA-APQ8-200921/2394
Integer Underflow (Wrap or Wraparound)	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.com/company/product-security/bulletins/august-2021-bulletin	O-QUA-APQ8-200921/2395

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Voice & Music, Snapdragon Wearables **CVE ID : CVE-2021-1919**		
Integer Underflow (Wrap or Wraparound)	08-Sep-21	10	Integer underflow can occur due to improper 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.com/company/product-security/bulletins/august-2021-bulletin	O-QUA-APQ8-200921/2396
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	08-Sep-21	10	Possible buffer overflow due to 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 Networking **CVE ID : CVE-2021-1972**	https://www.qualcomm.com/company/product-security/bulletins/august-2021-bulletin	O-QUA-APQ8-200921/2397
apq8037_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,	https://www.qualcomm.com/company/product-security/bulletins/august-2021-bulletin	O-QUA-APQ8-200921/2398

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.com/company/product-security/bulletins/august-2021-bulletin	O-QUA-APQ8-200921/2399
Integer Underflow (Wrap or Wraparound)	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.com/company/product-security/bulletins/august-2021-bulletin	O-QUA-APQ8-200921/2400
Integer Underflow (Wrap or Wraparound)	08-Sep-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.com/company/product-security/bulletins/august-2021-bulletin	O-QUA-APQ8-200921/2401

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_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.com/company/product-security/bulletins/august-2021-bulletin	O-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.com/company/product-security/bulletins/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.com/company/product-security/bull	O-QUA-APQ8-200921/2404

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 Wraparound)	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.com/company/product-security/bulletins/august-2021-bulletin	O-QUA-APQ8-200921/2405
Integer Underflow (Wrap or Wraparound)	08-Sep-21	10	Integer underflow can occur due to improper 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.com/company/product-security/bulletins/august-2021-bulletin	O-QUA-APQ8-200921/2406
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.com/company/product-security/bulletins/august-	O-QUA-APQ8-200921/2407

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1928**	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 Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1972**	https://www.qualcomm.com/company/product-security/bulletins/august-2021-bulletin	O-QUA-APQ8-200921/2408
apq8064au_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.com/company/product-security/bulletins/august-2021-bulletin	O-QUA-APQ8-200921/2409
Buffer Copy	08-Sep-21	10	Possible buffer overflow due	https://www.	O-QUA-APQ8-

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 Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1972**	qualcomm.com/company/product-security/bulletins/august-2021-bulletin	200921/2410
apq8076_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.com/company/product-security/bulletins/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.com/company/product-security/bulletins/august-2021-bulletin	O-QUA-APQ8-200921/2412

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1972**		
apq8084_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.com/company/product-security/bulletins/august-2021-bulletin	O-QUA-APQ8-200921/2413
Integer Underflow (Wrap or Wraparound)	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.com/company/product-security/bulletins/august-2021-bulletin	O-QUA-APQ8-200921/2414
Integer Underflow (Wrap or Wraparound)	08-Sep-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.com/company/product-security/bulletins/august-2021-bulletin	O-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_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.com/company/product-security/bulletins/august-2021-bulletin	O-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.com/company/product-security/bulletins/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.com/company/product-security/bull	O-QUA-APQ8-200921/2418

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 Wraparound)	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.com/company/product-security/bulletins/august-2021-bulletin	O-QUA-APQ8-200921/2419
Integer Underflow (Wrap or Wraparound)	08-Sep-21	10	Integer underflow can occur due to improper 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.com/company/product-security/bulletins/august-2021-bulletin	O-QUA-APQ8-200921/2420
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.com/company/product-security/bulletins/august-	O-QUA-APQ8-200921/2421

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wearables **CVE ID : CVE-2021-1929**	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 Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1972**	https://www.qualcomm.com/company/product-security/bulletins/august-2021-bulletin	O-QUA-APQ8-200921/2422
aqt1000_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.com/company/product-security/bulletins/august-2021-bulletin	O-QUA-AQT1-200921/2423
Loop with Unreachable Exit	08-Sep-21	5	Loop with unreachable exit condition may occur due to improper handling of	https://www.qualcomm.com/company/	O-QUA-AQT1-200921/2424

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/bulletins/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.com/company/product-security/bulletins/august-2021-bulletin	O-QUA-AQT1-200921/2425
Integer Underflow (Wrap or Wraparound)	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.com/company/product-security/bulletins/august-2021-bulletin	O-QUA-AQT1-200921/2426
Integer Underflow (Wrap or	08-Sep-21	10	Integer underflow can occur due to improper handling of incoming RTCP packets in	https://www.qualcomm.com/company/	O-QUA-AQT1-200921/2427

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Wraparound)			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/bulletins/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.com/company/product-security/bulletins/august-2021-bulletin	O-QUA-AQT1-200921/2428
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.com/company/product-security/bulletins/august-2021-bulletin	O-QUA-AQT1-200921/2429
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.com/company/product-security/bulletins/august-2021-bulletin	O-QUA-AQT1-200921/2430

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 Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1972**	https://www.qualcomm.com/company/product-security/bulletins/august-2021-bulletin	O-QUA-AQT1-200921/2431
ar6003_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.com/company/product-security/bulletins/august-2021-bulletin	O-QUA-AR60-200921/2432
Integer Underflow (Wrap or Wraparound)	08-Sep-21	10	Integer 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.com/company/product-security/bulletins/august-2021-bulletin	O-QUA-AR60-200921/2433

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 Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1972**	https://www.qualcomm.com/company/product-security/bulletins/august-2021-bulletin	O-QUA-AR60-200921/2434
ar7420_firmware					
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	08-Sep-21	10	Possible buffer overflow due to 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 Networking **CVE ID : CVE-2021-1972**	https://www.qualcomm.com/company/product-security/bulletins/august-2021-bulletin	O-QUA-AR74-200921/2435
ar8031_firmware					
Exposure of Resource to	08-Sep-21	2.1	Child process can leak information from parent	https://www.qualcomm.co	O-QUA-AR80-

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/bulletins/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 Mobile, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1972**	https://www.qualcomm.com/company/product-security/bulletins/august-2021-bulletin	O-QUA-AR80-200921/2437
ar8035_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,	https://www.qualcomm.com/company/product-security/bulletins/august-2021-bulletin	O-QUA-AR80-200921/2438

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 Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1972**	https://www.qualcomm.com/company/product-security/bulletins/august-2021-bulletin	O-QUA-AR80-200921/2439
ar9380_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.com/company/product-security/bulletins/august-2021-bulletin	O-QUA-AR93-200921/2440
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.com/company/product-security/bulletins/august-	O-QUA-AR93-200921/2441

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	
csr6030_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.com/company/product-security/bulletins/august-2021-bulletin	O-QUA-CSR6-200921/2442
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.com/company/product-security/bulletins/august-2021-bulletin	O-QUA-CSR6-200921/2443
Out-of-	08-Sep-21	10	Possible buffer underflow	https://www.	O-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 **CVE ID : CVE-2021-1916**	qualcomm.com/company/product-security/bulletins/august-2021-bulletin	200921/2444
Integer Underflow (Wrap or Wraparound)	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.com/company/product-security/bulletins/august-2021-bulletin	O-QUA-CSR6-200921/2445
Integer Underflow (Wrap or Wraparound)	08-Sep-21	10	Integer underflow can occur due to improper 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.com/company/product-security/bulletins/august-2021-bulletin	O-QUA-CSR6-200921/2446
Buffer Copy without	08-Sep-21	10	Possible buffer overflow due to improper validation of	https://www.qualcomm.co	O-QUA-CSR6-200921/2447

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 Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1972**	m/company/product-security/bulletins/august-2021-bulletin	
csr8811_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.com/company/product-security/bulletins/august-2021-bulletin	O-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 Voice & Music, Snapdragon Wearables, Snapdragon Wired	https://www.qualcomm.com/company/product-security/bulletins/august-2021-bulletin	O-QUA-CSR8-200921/2449

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Infrastructure and Networking **CVE ID : CVE-2021-1972**		
csra6620_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.com/company/product-security/bulletins/august-2021-bulletin	O-QUA-CSRA-200921/2450
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	08-Sep-21	10	Possible buffer overflow due to 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 Networking **CVE ID : CVE-2021-1972**	https://www.qualcomm.com/company/product-security/bulletins/august-2021-bulletin	O-QUA-CSRA-200921/2451
csra6640_firmware					
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.com/company/product-	O-QUA-CSRA-200921/2452

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/bulletins/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 Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1972**	https://www.qualcomm.com/company/product-security/bulletins/august-2021-bulletin	O-QUA-CSRA-200921/2453
csrb31024_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,	https://www.qualcomm.com/company/product-security/bulletins/august-2021-bulletin	O-QUA-CSRB-200921/2454

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.com/company/product-security/bulletins/august-2021-bulletin	O-QUA-CSRB-200921/2455
Out-of-bounds Write	08-Sep-21	10	Possible buffer underflow due to lack of check for negative indices values when 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.com/company/product-security/bulletins/august-2021-bulletin	O-QUA-CSRB-200921/2456
Integer Underflow (Wrap or Wraparound)	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.com/company/product-security/bulletins/august-2021-bulletin	O-QUA-CSRB-200921/2457

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Wearables **CVE ID : CVE-2021-1919**		
Integer Underflow (Wrap or Wraparound)	08-Sep-21	10	Integer underflow can occur due to improper 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.com/company/product-security/bulletins/august-2021-bulletin	O-QUA-CSRB-200921/2458
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.com/company/product-security/bulletins/august-2021-bulletin	O-QUA-CSRB-200921/2459
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	08-Sep-21	10	Possible buffer overflow due to 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 Networking	https://www.qualcomm.com/company/product-security/bulletins/august-2021-bulletin	O-QUA-CSRB-200921/2460

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2021-1972		
fsm10055_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.com/company/product-security/bulletins/august-2021-bulletin	O-QUA-FSM1-200921/2461
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	08-Sep-21	10	Possible buffer overflow due to 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 Networking **CVE ID : CVE-2021-1972**	https://www.qualcomm.com/company/product-security/bulletins/august-2021-bulletin	O-QUA-FSM1-200921/2462
fsm10056_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,	https://www.qualcomm.com/company/product-security/bulletins/august-	O-QUA-FSM1-200921/2463

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	
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	08-Sep-21	10	Possible buffer overflow due to 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 Networking **CVE ID : CVE-2021-1972**	https://www.qualcomm.com/company/product-security/bulletins/august-2021-bulletin	O-QUA-FSM1-200921/2464
ipq4018_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.com/company/product-security/bulletins/august-2021-bulletin	O-QUA-IPQ4-200921/2465
Buffer Copy	08-Sep-21	10	Possible buffer overflow due	https://www.	O-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 Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1972**	qualcomm.com/company/product-security/bulletins/august-2021-bulletin	200921/2466
ipq4019_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.com/company/product-security/bulletins/august-2021-bulletin	O-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.com/company/product-security/bulletins/august-2021-bulletin	O-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_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.com/company/product-security/bulletins/august-2021-bulletin	O-QUA-IPQ4-200921/2469
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	08-Sep-21	10	Possible buffer overflow due to 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 Networking **CVE ID : CVE-2021-1972**	https://www.qualcomm.com/company/product-security/bulletins/august-2021-bulletin	O-QUA-IPQ4-200921/2470
ipq4029_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.com/company/product-	O-QUA-IPQ4-200921/2471

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/bulletins/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 Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1972**	https://www.qualcomm.com/company/product-security/bulletins/august-2021-bulletin	O-QUA-IPQ4-200921/2472
ipq5010_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.com/company/product-security/bulletins/august-2021-bulletin	O-QUA-IPQ5-200921/2473

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 Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1972**	https://www.qualcomm.com/company/product-security/bulletins/august-2021-bulletin	O-QUA-IPQ5-200921/2474
ipq5018_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.com/company/product-security/bulletins/august-2021-bulletin	O-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.com/company/product-security/bulletins/august-2021-bulletin	O-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_firmware					
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	08-Sep-21	10	Possible buffer overflow due to 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 Networking **CVE ID : CVE-2021-1972**	https://www.qualcomm.com/company/product-security/bulletins/august-2021-bulletin	O-QUA-IPQ5-200921/2477
ipq6000_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.com/company/product-security/bulletins/august-2021-bulletin	O-QUA-IPQ6-200921/2478
Buffer Copy without Checking	08-Sep-21	10	Possible buffer overflow due to improper validation of device types during P2P	https://www.qualcomm.com/company/	O-QUA-IPQ6-200921/2479

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/bulletins/august-2021-bulletin	
ipq6005_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.com/company/product-security/bulletins/august-2021-bulletin	O-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 Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and	https://www.qualcomm.com/company/product-security/bulletins/august-2021-bulletin	O-QUA-IPQ6-200921/2481

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Networking **CVE ID : CVE-2021-1972**		
ipq6010_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.com/company/product-security/bulletins/august-2021-bulletin	O-QUA-IPQ6-200921/2482
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	08-Sep-21	10	Possible buffer overflow due to 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 Networking **CVE ID : CVE-2021-1972**	https://www.qualcomm.com/company/product-security/bulletins/august-2021-bulletin	O-QUA-IPQ6-200921/2483
ipq6018_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	https://www.qualcomm.com/company/product-security/bulletins/august-	O-QUA-IPQ6-200921/2484

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1928**	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 Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1972**	https://www.qualcomm.com/company/product-security/bulletins/august-2021-bulletin	O-QUA-IPQ6-200921/2485
ipq6028_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.com/company/product-security/bulletins/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	O-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 Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1972**	m/company/product-security/bulletins/august-2021-bulletin	
ipq8064_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.com/company/product-security/bulletins/august-2021-bulletin	O-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 Voice & Music, Snapdragon Wearables, Snapdragon Wired	https://www.qualcomm.com/company/product-security/bulletins/august-2021-bulletin	O-QUA-IPQ8-200921/2489

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Infrastructure and Networking **CVE ID : CVE-2021-1972**		
ipq8065_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.com/company/product-security/bulletins/august-2021-bulletin	O-QUA-IPQ8-200921/2490
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	08-Sep-21	10	Possible buffer overflow due to 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 Networking **CVE ID : CVE-2021-1972**	https://www.qualcomm.com/company/product-security/bulletins/august-2021-bulletin	O-QUA-IPQ8-200921/2491
ipq8068_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.com/company/product-security/bull	O-QUA-IPQ8-200921/2492

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 Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1972**	https://www.qualcomm.com/company/product-security/bulletins/august-2021-bulletin	O-QUA-IPQ8-200921/2493
ipq8069_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.com/company/product-security/bulletins/august-2021-bulletin	O-QUA-IPQ8-200921/2494
Buffer Copy	08-Sep-21	10	Possible buffer overflow due	https://www.	O-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 Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1972**	qualcomm.com/company/product-security/bulletins/august-2021-bulletin	200921/2495
ipq8070a_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.com/company/product-security/bulletins/august-2021-bulletin	O-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.com/company/product-security/bulletins/august-2021-bulletin	O-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_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.com/company/product-security/bulletins/august-2021-bulletin	O-QUA-IPQ8-200921/2498
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	08-Sep-21	10	Possible buffer overflow due to 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 Networking **CVE ID : CVE-2021-1972**	https://www.qualcomm.com/company/product-security/bulletins/august-2021-bulletin	O-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.com/company/product-	O-QUA-IPQ8-200921/2500

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/bulletins/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 Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1972**	https://www.qualcomm.com/company/product-security/bulletins/august-2021-bulletin	O-QUA-IPQ8-200921/2501
ipq8071_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.com/company/product-security/bulletins/august-2021-bulletin	O-QUA-IPQ8-200921/2502

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 Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1972**	https://www.qualcomm.com/company/product-security/bulletins/august-2021-bulletin	O-QUA-IPQ8-200921/2503
ipq8072a_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.com/company/product-security/bulletins/august-2021-bulletin	O-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.com/company/product-security/bulletins/august-2021-bulletin	O-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_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.com/company/product-security/bulletins/august-2021-bulletin	O-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 Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1972**	https://www.qualcomm.com/company/product-security/bulletins/august-2021-bulletin	O-QUA-IPQ8-200921/2507
ipq8074a_firmware					
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.com/company/	O-QUA-IPQ8-200921/2508

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/bulletins/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 Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1972**	https://www.qualcomm.com/company/product-security/bulletins/august-2021-bulletin	O-QUA-IPQ8-200921/2509
ipq8074_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.com/company/product-security/bulletins/august-2021-bulletin	O-QUA-IPQ8-200921/2510

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 Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1972**	https://www.qualcomm.com/company/product-security/bulletins/august-2021-bulletin	O-QUA-IPQ8-200921/2511
ipq8076a_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.com/company/product-security/bulletins/august-2021-bulletin	O-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.com/company/product-security/bulletins/august-2021-bulletin	O-QUA-IPQ8-200921/2513

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_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.com/company/product-security/bulletins/august-2021-bulletin	O-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 Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1972**	https://www.qualcomm.com/company/product-security/bulletins/august-2021-bulletin	O-QUA-IPQ8-200921/2515
ipq8078a_firmware					

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.com/company/product-security/bulletins/august-2021-bulletin	O-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 Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1972**	https://www.qualcomm.com/company/product-security/bulletins/august-2021-bulletin	O-QUA-IPQ8-200921/2517
ipq8078_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	https://www.qualcomm.com/company/product-security/bulletins/august-2021-bulletin	O-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 Mobile, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1972**	https://www.qualcomm.com/company/product-security/bulletins/august-2021-bulletin	O-QUA-IPQ8-200921/2519
ipq8173_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.com/company/product-security/bulletins/august-2021-bulletin	O-QUA-IPQ8-200921/2520
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.com/company/product-security/bulletins/august-	O-QUA-IPQ8-200921/2521

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_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.com/company/product-security/bulletins/august-2021-bulletin	O-QUA-IPQ8-200921/2522
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	08-Sep-21	10	Possible buffer overflow due to 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 Networking **CVE ID : CVE-2021-1972**	https://www.qualcomm.com/company/product-security/bulletins/august-2021-bulletin	O-QUA-IPQ8-200921/2523

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
mdm8207_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.com/company/product-security/bulletins/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.com/company/product-security/bulletins/august-2021-bulletin	O-QUA-MDM8-200921/2525
Integer Underflow (Wrap or Wraparound)	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.com/company/product-security/bulletins/august-2021-bulletin	O-QUA-MDM8-200921/2526

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2021-1919		
Integer Underflow (Wrap or Wraparound)	08-Sep-21	10	Integer underflow can occur due to improper 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.com/company/product-security/bulletins/august-2021-bulletin	O-QUA-MDM8-200921/2527
mdm8215m_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.com/company/product-security/bulletins/august-2021-bulletin	O-QUA-MDM8-200921/2528
Integer Underflow (Wrap or Wraparound)	08-Sep-21	10	Integer underflow can occur due to improper 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.com/company/product-security/bulletins/august-2021-bulletin	O-QUA-MDM8-200921/2529

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 Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1972**	https://www.qualcomm.com/company/product-security/bulletins/august-2021-bulletin	O-QUA-MDM8-200921/2530
mdm8215_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.com/company/product-security/bulletins/august-2021-bulletin	O-QUA-MDM8-200921/2531
Integer Underflow (Wrap or Wraparound)	08-Sep-21	10	Integer 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.com/company/product-security/bulletins/august-2021-bulletin	O-QUA-MDM8-200921/2532

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 Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1972**	https://www.qualcomm.com/company/product-security/bulletins/august-2021-bulletin	O-QUA-MDM8-200921/2533
mdm8615m_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.com/company/product-security/bulletins/august-2021-bulletin	O-QUA-MDM8-200921/2534
Integer Underflow (Wrap or Wraparound)	08-Sep-21	10	Integer underflow can occur due to improper handling of incoming RTCP packets in Snapdragon Auto, Snapdragon Compute,	https://www.qualcomm.com/company/product-security/bull	O-QUA-MDM8-200921/2535

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-2021-1920**	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 Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1972**	https://www.qualcomm.com/company/product-security/bulletins/august-2021-bulletin	O-QUA-MDM8-200921/2536
mdm9150_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.com/company/product-security/bulletins/august-2021-bulletin	O-QUA-MDM9-200921/2537
Loop with	08-Sep-21	5	Loop with unreachable exit	https://www.	O-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 **CVE ID : CVE-2021-1914**	qualcomm.com/company/product-security/bulletins/august-2021-bulletin	MDM9-200921/2538
Out-of-bounds Write	08-Sep-21	10	Possible buffer underflow due to lack of check for negative indices values when 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.com/company/product-security/bulletins/august-2021-bulletin	O-QUA-MDM9-200921/2539
Integer Underflow (Wrap or Wraparound)	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.com/company/product-security/bulletins/august-2021-bulletin	O-QUA-MDM9-200921/2540
Integer	08-Sep-21	10	Integer underflow can occur	https://www.	O-QUA-

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Underflow (Wrap or Wraparound)			due to improper 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.com/company/product-security/bulletins/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 Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1972**	https://www.qualcomm.com/company/product-security/bulletins/august-2021-bulletin	O-QUA-MDM9-200921/2542
mdm9205_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	https://www.qualcomm.com/company/product-security/bulletins/august-2021-bulletin	O-QUA-MDM9-200921/2543

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 **CVE ID : CVE-2021-1916**	https://www.qualcomm.com/company/product-security/bulletins/august-2021-bulletin	O-QUA-MDM9-200921/2544
Integer Underflow (Wrap or Wraparound)	08-Sep-21	10	Integer underflow can occur due to improper 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.com/company/product-security/bulletins/august-2021-bulletin	O-QUA-MDM9-200921/2545
mdm9206_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,	https://www.qualcomm.com/company/product-security/bulletins/august-2021-bulletin	O-QUA-MDM9-200921/2546

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.com/company/product-security/bulletins/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.com/company/product-security/bulletins/august-2021-bulletin	O-QUA-MDM9-200921/2548
Integer Underflow (Wrap or Wraparound)	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.com/company/product-security/bulletins/august-2021-bulletin	O-QUA-MDM9-200921/2549

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 Wraparound)	08-Sep-21	10	Integer underflow can occur due to improper 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.com/company/product-security/bulletins/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.com/company/product-security/bulletins/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.com/company/product-security/bulletins/august-2021-bulletin	O-QUA-MDM9-200921/2552

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_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.com/company/product-security/bulletins/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.com/company/product-security/bulletins/august-2021-bulletin	O-QUA-MDM9-200921/2554
Integer Underflow (Wrap or Wraparound)	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.com/company/product-security/bull	O-QUA-MDM9-200921/2555

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-2021-1919**	etins/august-2021-bulletin	
Integer Underflow (Wrap or Wraparound)	08-Sep-21	10	Integer underflow can occur due to improper 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.com/company/product-security/bulletins/august-2021-bulletin	O-QUA-MDM9-200921/2556
mdm9215_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.com/company/product-security/bulletins/august-2021-bulletin	O-QUA-MDM9-200921/2557
Integer Underflow (Wrap or Wraparound)	08-Sep-21	10	Integer underflow can occur due to improper handling of incoming RTCP packets in Snapdragon Auto, Snapdragon Compute,	https://www.qualcomm.com/company/product-security/bull	O-QUA-MDM9-200921/2558

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-2021-1920**	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 Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1972**	https://www.qualcomm.com/company/product-security/bulletins/august-2021-bulletin	O-QUA-MDM9-200921/2559
mdm9230_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.com/company/product-security/bulletins/august-2021-bulletin	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-

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
(Wrap or Wraparound)			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/bulletins/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 Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1972**	https://www.qualcomm.com/company/product-security/bulletins/august-2021-bulletin	O-QUA-MDM9-200921/2562
mdm9250_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,	https://www.qualcomm.com/company/product-security/bulletins/august-2021-bulletin	O-QUA-MDM9-200921/2563

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.com/company/product-security/bulletins/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.com/company/product-security/bulletins/august-2021-bulletin	O-QUA-MDM9-200921/2565
Integer Underflow (Wrap or Wraparound)	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.com/company/product-security/bulletins/august-2021-bulletin	O-QUA-MDM9-200921/2566

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Wearables **CVE ID : CVE-2021-1919**		
Integer Underflow (Wrap or Wraparound)	08-Sep-21	10	Integer underflow can occur due to improper 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.com/company/product-security/bulletins/august-2021-bulletin	O-QUA-MDM9-200921/2567
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	08-Sep-21	10	Possible buffer overflow due to 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 Networking **CVE ID : CVE-2021-1972**	https://www.qualcomm.com/company/product-security/bulletins/august-2021-bulletin	O-QUA-MDM9-200921/2568
mdm9310_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,	https://www.qualcomm.com/company/product-security/bulletins/august-2021-bulletin	O-QUA-MDM9-200921/2569

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 Wraparound)	08-Sep-21	10	Integer underflow can occur due to improper 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.com/company/product-security/bulletins/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 Mobile, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1972**	https://www.qualcomm.com/company/product-security/bulletins/august-2021-bulletin	O-QUA-MDM9-200921/2571
mdm9330_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,	https://www.qualcomm.com/company/product-security/bull	O-QUA-MDM9-200921/2572

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 Wraparound)	08-Sep-21	10	Integer underflow can occur due to improper 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.com/company/product-security/bulletins/august-2021-bulletin	O-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 Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1972**	https://www.qualcomm.com/company/product-security/bulletins/august-2021-bulletin	O-QUA-MDM9-200921/2574
mdm9607_firmware					
Exposure of Resource to	08-Sep-21	2.1	Child process can leak information from parent	https://www.qualcomm.co	O-QUA-MDM9-

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/bulletins/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.com/company/product-security/bulletins/august-2021-bulletin	O-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.com/company/product-security/bulletins/august-2021-bulletin	O-QUA-MDM9-200921/2577

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Integer Underflow (Wrap or Wraparound)	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.com/company/product-security/bulletins/august-2021-bulletin	O-QUA-MDM9-200921/2578
Integer Underflow (Wrap or Wraparound)	08-Sep-21	10	Integer underflow can occur due to improper 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.com/company/product-security/bulletins/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 Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking	https://www.qualcomm.com/company/product-security/bulletins/august-2021-bulletin	O-QUA-MDM9-200921/2580

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2021-1972		
mdm9615m_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.com/company/product-security/bulletins/august-2021-bulletin	O-QUA-MDM9-200921/2581
Integer Underflow (Wrap or Wraparound)	08-Sep-21	10	Integer underflow can occur due to improper 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.com/company/product-security/bulletins/august-2021-bulletin	O-QUA-MDM9-200921/2582
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	08-Sep-21	10	Possible buffer overflow due to 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.com/company/product-security/bulletins/august-2021-bulletin	O-QUA-MDM9-200921/2583

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1972**		
mdm9615_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.com/company/product-security/bulletins/august-2021-bulletin	O-QUA-MDM9-200921/2584
Integer Underflow (Wrap or Wraparound)	08-Sep-21	10	Integer underflow can occur due to improper 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.com/company/product-security/bulletins/august-2021-bulletin	O-QUA-MDM9-200921/2585
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	08-Sep-21	10	Possible buffer 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.com/company/product-security/bulletins/august-2021-bulletin	O-QUA-MDM9-200921/2586

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_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.com/company/product-security/bulletins/august-2021-bulletin	O-QUA-MDM9-200921/2587
Integer Underflow (Wrap or Wraparound)	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.com/company/product-security/bulletins/august-2021-bulletin	O-QUA-MDM9-200921/2588
Integer Underflow (Wrap or Wraparound)	08-Sep-21	10	Integer underflow can occur due to improper handling of incoming RTCP packets in Snapdragon Auto, Snapdragon Compute,	https://www.qualcomm.com/company/product-security/bull	O-QUA-MDM9-200921/2589

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-2021-1920**	etins/august-2021-bulletin	
mdm9626_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.com/company/product-security/bulletins/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 Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1972**	https://www.qualcomm.com/company/product-security/bulletins/august-2021-bulletin	O-QUA-MDM9-200921/2591
mdm9628_firmware					

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.com/company/product-security/bulletins/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 IoT, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2021-1914**	https://www.qualcomm.com/company/product-security/bulletins/august-2021-bulletin	O-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.com/company/product-security/bulletins/august-2021-bulletin	O-QUA-MDM9-200921/2594

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2021-1916		
Integer Underflow (Wrap or Wraparound)	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.com/company/product-security/bulletins/august-2021-bulletin	O-QUA-MDM9-200921/2595
Integer Underflow (Wrap or Wraparound)	08-Sep-21	10	Integer underflow can occur due to improper 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.com/company/product-security/bulletins/august-2021-bulletin	O-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 Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and	https://www.qualcomm.com/company/product-security/bulletins/august-2021-bulletin	O-QUA-MDM9-200921/2597

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Networking **CVE ID : CVE-2021-1972**		
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 **CVE ID : CVE-2021-1916**	https://www.qualcomm.com/company/product-security/bulletins/august-2021-bulletin	O-QUA-MDM9-200921/2598
Integer Underflow (Wrap or Wraparound)	08-Sep-21	10	Integer underflow can occur due to improper 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.com/company/product-security/bulletins/august-2021-bulletin	O-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.com/company/product-security/bulletins/august-2021-bulletin	O-QUA-MDM9-200921/2600

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.com/company/product-security/bulletins/august-2021-bulletin	O-QUA-MDM9-200921/2601
Integer Underflow (Wrap or Wraparound)	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.com/company/product-security/bulletins/august-2021-bulletin	O-QUA-MDM9-200921/2602
Integer Underflow (Wrap or Wraparound)	08-Sep-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.com/company/product-security/bulletins/august-2021-bulletin	O-QUA-MDM9-200921/2603

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_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.com/company/product-security/bulletins/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.com/company/product-security/bulletins/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.com/company/product-security/bull	O-QUA-MDM9-200921/2606

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 Wraparound)	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.com/company/product-security/bulletins/august-2021-bulletin	O-QUA-MDM9-200921/2607
Integer Underflow (Wrap or Wraparound)	08-Sep-21	10	Integer underflow can occur due to improper 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.com/company/product-security/bulletins/august-2021-bulletin	O-QUA-MDM9-200921/2608
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.com/company/product-security/bulletins/august-	O-QUA-MDM9-200921/2609

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_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.com/company/product-security/bulletins/august-2021-bulletin	O-QUA-MDM9-200921/2610
Integer Underflow (Wrap or Wraparound)	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.com/company/product-security/bulletins/august-2021-bulletin	O-QUA-MDM9-200921/2611
Integer Underflow (Wrap or	08-Sep-21	10	Integer underflow can occur due to improper handling of incoming RTCP packets in	https://www.qualcomm.com/company/	O-QUA-MDM9-200921/2612

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Wraparound)			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/bulletins/august-2021-bulletin	
mdm9650_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.com/company/product-security/bulletins/august-2021-bulletin	O-QUA-MDM9-200921/2613
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.com/company/product-security/bulletins/august-2021-bulletin	O-QUA-MDM9-200921/2614
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.com/company/product-security/bulletins/august-2021-bulletin	MDM9-200921/2615
Integer Underflow (Wrap or Wraparound)	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.com/company/product-security/bulletins/august-2021-bulletin	O-QUA-MDM9-200921/2616
Integer Underflow (Wrap or Wraparound)	08-Sep-21	10	Integer underflow can occur due to improper 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.com/company/product-security/bulletins/august-2021-bulletin	O-QUA-MDM9-200921/2617
Buffer Copy without	08-Sep-21	10	Possible buffer overflow due to improper validation of	https://www.qualcomm.co	O-QUA-MDM9-

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 Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1972**	m/company/product-security/bulletins/august-2021-bulletin	200921/2618
mdm9655_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.com/company/product-security/bulletins/august-2021-bulletin	O-QUA-MDM9-200921/2619
Integer Underflow (Wrap or Wraparound)	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.com/company/product-security/bulletins/august-2021-bulletin	O-QUA-MDM9-200921/2620

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2021-1919		
Integer Underflow (Wrap or Wraparound)	08-Sep-21	10	Integer underflow can occur due to improper 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.com/company/product-security/bulletins/august-2021-bulletin	O-QUA-MDM9-200921/2621
msm8108_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.com/company/product-security/bulletins/august-2021-bulletin	O-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.com/company/product-security/bulletins/august-2021-bulletin	O-QUA-MSM8-200921/2623

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Wearables **CVE ID : CVE-2021-1916**		
Integer Underflow (Wrap or Wraparound)	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.com/company/product-security/bulletins/august-2021-bulletin	O-QUA-MSM8-200921/2624
Integer Underflow (Wrap or Wraparound)	08-Sep-21	10	Integer underflow can occur due to improper 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.com/company/product-security/bulletins/august-2021-bulletin	O-QUA-MSM8-200921/2625
msm8208_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	https://www.qualcomm.com/company/product-security/bulletins/august-2021-bulletin	O-QUA-MSM8-200921/2626

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 **CVE ID : CVE-2021-1916**	https://www.qualcomm.com/company/product-security/bulletins/august-2021-bulletin	O-QUA-MSM8-200921/2627
Integer Underflow (Wrap or Wraparound)	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.com/company/product-security/bulletins/august-2021-bulletin	O-QUA-MSM8-200921/2628
Integer Underflow (Wrap or Wraparound)	08-Sep-21	10	Integer underflow can occur due to improper 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.com/company/product-security/bulletins/august-2021-bulletin	O-QUA-MSM8-200921/2629

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2021-1920		
msm8209_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.com/company/product-security/bulletins/august-2021-bulletin	O-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.com/company/product-security/bulletins/august-2021-bulletin	O-QUA-MSM8-200921/2631
Integer Underflow (Wrap or Wraparound)	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.com/company/product-security/bulletins/august-2021-bulletin	O-QUA-MSM8-200921/2632

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Wearables **CVE ID : CVE-2021-1919**		
Integer Underflow (Wrap or Wraparound)	08-Sep-21	10	Integer underflow can occur due to improper 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.com/company/product-security/bulletins/august-2021-bulletin	O-QUA-MSM8-200921/2633
msm8608_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.com/company/product-security/bulletins/august-2021-bulletin	O-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.com/company/product-security/bulletins/august-2021-bulletin	O-QUA-MSM8-200921/2635

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Voice & Music, Snapdragon Wearables **CVE ID : CVE-2021-1916**		
Integer Underflow (Wrap or Wraparound)	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.com/company/product-security/bulletins/august-2021-bulletin	O-QUA-MSM8-200921/2636
Integer Underflow (Wrap or Wraparound)	08-Sep-21	10	Integer underflow can occur due to improper 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.com/company/product-security/bulletins/august-2021-bulletin	O-QUA-MSM8-200921/2637
msm8909w_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,	https://www.qualcomm.com/company/product-security/bulletins/august-2021-bulletin	O-QUA-MSM8-200921/2638

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.com/company/product-security/bulletins/august-2021-bulletin	O-QUA-MSM8-200921/2639
Out-of-bounds Write	08-Sep-21	10	Possible buffer underflow due to lack of check for negative indices values when 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.com/company/product-security/bulletins/august-2021-bulletin	O-QUA-MSM8-200921/2640
Integer Underflow (Wrap or Wraparound)	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.com/company/product-security/bulletins/august-2021-bulletin	O-QUA-MSM8-200921/2641

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 Wraparound)	08-Sep-21	10	Integer underflow can occur due to improper 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.com/company/product-security/bulletins/august-2021-bulletin	O-QUA-MSM8-200921/2642
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	08-Sep-21	10	Possible buffer overflow due to 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 Networking **CVE ID : CVE-2021-1972**	https://www.qualcomm.com/company/product-security/bulletins/august-2021-bulletin	O-QUA-MSM8-200921/2643
msm8917_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,	https://www.qualcomm.com/company/product-security/bulletins/august-	O-QUA-MSM8-200921/2644

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	
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.com/company/product-security/bulletins/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.com/company/product-security/bulletins/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.com/company/product-	O-QUA-MSM8-200921/2647

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/bulletins/august-2021-bulletin	
Integer Underflow (Wrap or Wraparound)	08-Sep-21	10	Integer underflow can occur due to improper 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.com/company/product-security/bulletins/august-2021-bulletin	O-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 Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1972**	https://www.qualcomm.com/company/product-security/bulletins/august-2021-bulletin	O-QUA-MSM8-200921/2649
msm8920_firmware					
Loop with Unreachable	08-Sep-21	5	Loop with unreachable exit condition may occur due to	https://www.qualcomm.co	O-QUA-MSM8-

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/bulletins/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.com/company/product-security/bulletins/august-2021-bulletin	O-QUA-MSM8-200921/2651
Integer Underflow (Wrap or Wraparound)	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.com/company/product-security/bulletins/august-2021-bulletin	O-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-

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
(Wrap or Wraparound)			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/bulletins/august-2021-bulletin	200921/2653
msm8937_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.com/company/product-security/bulletins/august-2021-bulletin	O-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.com/company/product-security/bulletins/august-2021-bulletin	O-QUA-MSM8-200921/2655
Integer	08-Sep-21	10	Integer underflow can occur	https://www.	O-QUA-

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Underflow (Wrap or Wraparound)			when 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.com/company/product-security/bulletins/august-2021-bulletin	MSM8-200921/2656
Integer Underflow (Wrap or Wraparound)	08-Sep-21	10	Integer underflow can occur due to improper 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.com/company/product-security/bulletins/august-2021-bulletin	O-QUA-MSM8-200921/2657
msm8940_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.com/company/product-security/bulletins/august-2021-bulletin	O-QUA-MSM8-200921/2658
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.com/company/product-security/bulletins/august-2021-bulletin	MSM8-200921/2659
Integer Underflow (Wrap or Wraparound)	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.com/company/product-security/bulletins/august-2021-bulletin	O-QUA-MSM8-200921/2660
Integer Underflow (Wrap or Wraparound)	08-Sep-21	10	Integer underflow can occur due to improper 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.com/company/product-security/bulletins/august-2021-bulletin	O-QUA-MSM8-200921/2661
msm8953_firmware					
Exposure of	08-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 Voice & Music, Snapdragon Wearables **CVE ID : CVE-2021-1904**	qualcomm.com/company/product-security/bulletins/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.com/company/product-security/bulletins/august-2021-bulletin	O-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.com/company/product-security/bulletins/august-2021-bulletin	O-QUA-MSM8-200921/2664

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2021-1916		
Integer Underflow (Wrap or Wraparound)	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.com/company/product-security/bulletins/august-2021-bulletin	O-QUA-MSM8-200921/2665
Integer Underflow (Wrap or Wraparound)	08-Sep-21	10	Integer underflow can occur due to improper 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.com/company/product-security/bulletins/august-2021-bulletin	O-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 Mobile, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and	https://www.qualcomm.com/company/product-security/bulletins/august-2021-bulletin	O-QUA-MSM8-200921/2667

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.com/company/product-security/bulletins/august-2021-bulletin	O-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.com/company/product-security/bulletins/august-2021-bulletin	O-QUA-MSM8-200921/2669
Integer Underflow (Wrap or Wraparound)	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.com/company/product-security/bulletins/august-2021-bulletin	O-QUA-MSM8-200921/2670

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Voice & Music, Snapdragon Wearables **CVE ID : CVE-2021-1919**		
Integer Underflow (Wrap or Wraparound)	08-Sep-21	10	Integer underflow can occur due to improper 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.com/company/product-security/bulletins/august-2021-bulletin	O-QUA-MSM8-200921/2671
msm8976_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.com/company/product-security/bulletins/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.com/company/product-security/bulletins/august-2021-bulletin	O-QUA-MSM8-200921/2673

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 Wraparound)	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.com/company/product-security/bulletins/august-2021-bulletin	O-QUA-MSM8-200921/2674
Integer Underflow (Wrap or Wraparound)	08-Sep-21	10	Integer underflow can occur due to improper 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.com/company/product-security/bulletins/august-2021-bulletin	O-QUA-MSM8-200921/2675
msm8996au_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,	https://www.qualcomm.com/company/product-security/bulletins/august-2021-bulletin	O-QUA-MSM8-200921/2676

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 **CVE ID : CVE-2021-1914**	https://www.qualcomm.com/company/product-security/bulletins/august-2021-bulletin	O-QUA-MSM8-200921/2677
Out-of-bounds Write	08-Sep-21	10	Possible buffer underflow due to lack of check for negative indices values when 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.com/company/product-security/bulletins/august-2021-bulletin	O-QUA-MSM8-200921/2678
Integer Underflow (Wrap or Wraparound)	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.com/company/product-security/bulletins/august-2021-bulletin	O-QUA-MSM8-200921/2679

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 Wraparound)	08-Sep-21	10	Integer underflow can occur due to improper 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.com/company/product-security/bulletins/august-2021-bulletin	O-QUA-MSM8-200921/2680
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.com/company/product-security/bulletins/august-2021-bulletin	O-QUA-MSM8-200921/2681
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	08-Sep-21	10	Possible buffer overflow due to 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.com/company/product-security/bulletins/august-2021-bulletin	O-QUA-MSM8-200921/2682

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1972**		
pmp8074_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.com/company/product-security/bulletins/august-2021-bulletin	O-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 Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1972**	https://www.qualcomm.com/company/product-security/bulletins/august-2021-bulletin	O-QUA-PMP8-200921/2684
qca1990_firmware					
Out-of-bounds	08-Sep-21	10	Possible buffer underflow due to lack of check for negative indices values when	https://www.qualcomm.com/company/	O-QUA-QCA1-200921/2685

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/bulletins/august-2021-bulletin	
Integer Underflow (Wrap or Wraparound)	08-Sep-21	10	Integer underflow can occur due to improper 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.com/company/product-security/bulletins/august-2021-bulletin	O-QUA-QCA1-200921/2686
qca4004_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.com/company/product-security/bulletins/august-2021-bulletin	O-QUA-QCA4-200921/2687
Out-of-bounds	08-Sep-21	10	Possible buffer underflow due to lack of check for	https://www.qualcomm.co	O-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/bulletins/august-2021-bulletin	
Integer Underflow (Wrap or Wraparound)	08-Sep-21	10	Integer underflow can occur due to improper 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.com/company/product-security/bulletins/august-2021-bulletin	O-QUA-QCA4-200921/2689
qca4020_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.com/company/product-security/bulletins/august-2021-bulletin	O-QUA-QCA4-200921/2690

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 Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1972**	https://www.qualcomm.com/company/product-security/bulletins/august-2021-bulletin	O-QUA-QCA4-200921/2691
qca4024_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.com/company/product-security/bulletins/august-2021-bulletin	O-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.com/company/product-security/bulletins/august-2021-bulletin	O-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_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.com/company/product-security/bulletins/august-2021-bulletin	O-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.com/company/product-security/bulletins/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.com/company/product-security/bull	O-QUA-QCA6-200921/2696

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 Wraparound)	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.com/company/product-security/bulletins/august-2021-bulletin	O-QUA-QCA6-200921/2697
Integer Underflow (Wrap or Wraparound)	08-Sep-21	10	Integer underflow can occur due to improper 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.com/company/product-security/bulletins/august-2021-bulletin	O-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.com/company/product-security/bulletins/august-	O-QUA-QCA6-200921/2699

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 Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1972**	https://www.qualcomm.com/company/product-security/bulletins/august-2021-bulletin	O-QUA-QCA6-200921/2700
qca6174_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.com/company/product-security/bulletins/august-2021-bulletin	O-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.com/company/product-	O-QUA-QCA6-200921/2702

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/bulletins/august-2021-bulletin	
Integer Underflow (Wrap or Wraparound)	08-Sep-21	10	Integer underflow can occur due to improper 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.com/company/product-security/bulletins/august-2021-bulletin	O-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 Mobile, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1972**	https://www.qualcomm.com/company/product-security/bulletins/august-2021-bulletin	O-QUA-QCA6-200921/2704
qca6310_firmware					
Exposure of	08-Sep-21	2.1	Child process can leak	https://www.	O-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 Voice & Music, Snapdragon Wearables **CVE ID : CVE-2021-1904**	qualcomm.com/company/product-security/bulletins/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.com/company/product-security/bulletins/august-2021-bulletin	O-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.com/company/product-security/bulletins/august-2021-bulletin	O-QUA-QCA6-200921/2707

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2021-1916		
Integer Underflow (Wrap or Wraparound)	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.com/company/product-security/bulletins/august-2021-bulletin	O-QUA-QCA6-200921/2708
Integer Underflow (Wrap or Wraparound)	08-Sep-21	10	Integer underflow can occur due to improper 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.com/company/product-security/bulletins/august-2021-bulletin	O-QUA-QCA6-200921/2709
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.com/company/product-security/bulletins/august-2021-bulletin	O-QUA-QCA6-200921/2710

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 Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1972**	https://www.qualcomm.com/company/product-security/bulletins/august-2021-bulletin	O-QUA-QCA6-200921/2711
qca6320_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.com/company/product-security/bulletins/august-2021-bulletin	O-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.com/company/product-security/bulletins/august-2021-bulletin	O-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 **CVE ID : CVE-2021-1916**	https://www.qualcomm.com/company/product-security/bulletins/august-2021-bulletin	O-QUA-QCA6-200921/2714
Integer Underflow (Wrap or Wraparound)	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.com/company/product-security/bulletins/august-2021-bulletin	O-QUA-QCA6-200921/2715
Integer Underflow (Wrap or Wraparound)	08-Sep-21	10	Integer underflow can occur 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.com/company/product-security/bulletins/august-2021-bulletin	O-QUA-QCA6-200921/2716

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.com/company/product-security/bulletins/august-2021-bulletin	O-QUA-QCA6-200921/2717
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	08-Sep-21	10	Possible buffer overflow due to 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 Networking **CVE ID : CVE-2021-1972**	https://www.qualcomm.com/company/product-security/bulletins/august-2021-bulletin	O-QUA-QCA6-200921/2718
qca6335_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,	https://www.qualcomm.com/company/product-security/bulletins/august-	O-QUA-QCA6-200921/2719

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	
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.com/company/product-security/bulletins/august-2021-bulletin	O-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.com/company/product-security/bulletins/august-2021-bulletin	O-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.com/company/product-	O-QUA-QCA6-200921/2722

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/bulletins/august-2021-bulletin	
Integer Underflow (Wrap or Wraparound)	08-Sep-21	10	Integer underflow can occur due to improper 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.com/company/product-security/bulletins/august-2021-bulletin	O-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.com/company/product-security/bulletins/august-2021-bulletin	O-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.com/company/product-security/bull	O-QUA-QCA6-200921/2725

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_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.com/company/product-security/bulletins/august-2021-bulletin	O-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.com/company/product-security/bulletins/august-2021-bulletin	O-QUA-QCA6-200921/2727

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.com/company/product-security/bulletins/august-2021-bulletin	O-QUA-QCA6-200921/2728
Integer Underflow (Wrap or Wraparound)	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.com/company/product-security/bulletins/august-2021-bulletin	O-QUA-QCA6-200921/2729
Integer Underflow (Wrap or Wraparound)	08-Sep-21	10	Integer underflow can occur due to improper 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.com/company/product-security/bulletins/august-2021-bulletin	O-QUA-QCA6-200921/2730
Incorrect	08-Sep-21	4.6	Incorrect pointer argument	https://www.	O-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.com/company/product-security/bulletins/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.com/company/product-security/bulletins/august-2021-bulletin	O-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.com/company/product-security/bulletins/august-2021-bulletin	O-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.com/company/product-security/bulletins/august-2021-bulletin	O-QUA-QCA6-200921/2734

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_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.com/company/product-security/bulletins/august-2021-bulletin	O-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.com/company/product-security/bulletins/august-2021-bulletin	O-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.com/company/product-	O-QUA-QCA6-200921/2737

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/bulletins/august-2021-bulletin	
Integer Underflow (Wrap or Wraparound)	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.com/company/product-security/bulletins/august-2021-bulletin	O-QUA-QCA6-200921/2738
Integer Underflow (Wrap or Wraparound)	08-Sep-21	10	Integer underflow can occur due to improper 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.com/company/product-security/bulletins/august-2021-bulletin	O-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.com/company/product-security/bull	O-QUA-QCA6-200921/2740

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.com/company/product-security/bulletins/august-2021-bulletin	O-QUA-QCA6-200921/2741
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.com/company/product-security/bulletins/august-2021-bulletin	O-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 Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and	https://www.qualcomm.com/company/product-security/bulletins/august-2021-bulletin	O-QUA-QCA6-200921/2743

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Networking **CVE ID : CVE-2021-1972**		
qca6420_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.com/company/product-security/bulletins/august-2021-bulletin	O-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.com/company/product-security/bulletins/august-2021-bulletin	O-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.com/company/product-security/bulletins/august-2021-bulletin	O-QUA-QCA6-200921/2746

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 Wraparound)	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.com/company/product-security/bulletins/august-2021-bulletin	O-QUA-QCA6-200921/2747
Integer Underflow (Wrap or Wraparound)	08-Sep-21	10	Integer underflow can occur due to improper 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.com/company/product-security/bulletins/august-2021-bulletin	O-QUA-QCA6-200921/2748
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.com/company/product-security/bulletins/august-2021-bulletin	O-QUA-QCA6-200921/2749

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.com/company/product-security/bulletins/august-2021-bulletin	O-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.com/company/product-security/bulletins/august-2021-bulletin	O-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 Mobile, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1972**	https://www.qualcomm.com/company/product-security/bulletins/august-2021-bulletin	O-QUA-QCA6-200921/2752
qca6421_firmware					
Exposure of	08-Sep-21	2.1	Child process can leak	https://www.	O-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 Voice & Music, Snapdragon Wearables **CVE ID : CVE-2021-1904**	qualcomm.com/company/product-security/bulletins/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.com/company/product-security/bulletins/august-2021-bulletin	O-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.com/company/product-security/bulletins/august-2021-bulletin	O-QUA-QCA6-200921/2755

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2021-1916		
Integer Underflow (Wrap or Wraparound)	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.com/company/product-security/bulletins/august-2021-bulletin	O-QUA-QCA6-200921/2756
Integer Underflow (Wrap or Wraparound)	08-Sep-21	10	Integer underflow can occur due to improper 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.com/company/product-security/bulletins/august-2021-bulletin	O-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.com/company/product-security/bulletins/august-2021-bulletin	O-QUA-QCA6-200921/2758
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.com/company/product-	O-QUA-QCA6-200921/2759

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/bulletins/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.com/company/product-security/bulletins/august-2021-bulletin	O-QUA-QCA6-200921/2760
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	08-Sep-21	10	Possible buffer overflow due to 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 Networking **CVE ID : CVE-2021-1972**	https://www.qualcomm.com/company/product-security/bulletins/august-2021-bulletin	O-QUA-QCA6-200921/2761
qca6426_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	https://www.qualcomm.com/company/product-security/bull	O-QUA-QCA6-200921/2762

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.com/company/product-security/bulletins/august-2021-bulletin	O-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.com/company/product-security/bulletins/august-2021-bulletin	O-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.com/company/	O-QUA-QCA6-200921/2765

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Wraparound)			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/bulletins/august-2021-bulletin	
Integer Underflow (Wrap or Wraparound)	08-Sep-21	10	Integer underflow can occur due to improper 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.com/company/product-security/bulletins/august-2021-bulletin	O-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.com/company/product-security/bulletins/august-2021-bulletin	O-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.com/company/product-security/bulletins/august-2021-bulletin	O-QUA-QCA6-200921/2768

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.com/company/product-security/bulletins/august-2021-bulletin	O-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 Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1972**	https://www.qualcomm.com/company/product-security/bulletins/august-2021-bulletin	O-QUA-QCA6-200921/2770
qca6428_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	https://www.qualcomm.com/company/product-security/bulletins/august-2021-bulletin	O-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 Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1972**	https://www.qualcomm.com/company/product-security/bulletins/august-2021-bulletin	O-QUA-QCA6-200921/2772
qca6430_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.com/company/product-security/bulletins/august-2021-bulletin	O-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.com/company/product-	O-QUA-QCA6-200921/2774

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/bulletins/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.com/company/product-security/bulletins/august-2021-bulletin	O-QUA-QCA6-200921/2775
Integer Underflow (Wrap or Wraparound)	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.com/company/product-security/bulletins/august-2021-bulletin	O-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.com/company/product-	O-QUA-QCA6-200921/2777

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/bulletins/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.com/company/product-security/bulletins/august-2021-bulletin	O-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.com/company/product-security/bulletins/august-2021-bulletin	O-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.com/company/product-security/bulletins/august-2021-bulletin	O-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 Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1972**	https://www.qualcomm.com/company/product-security/bulletins/august-2021-bulletin	O-QUA-QCA6-200921/2781
qca6431_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.com/company/product-security/bulletins/august-2021-bulletin	O-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.com/company/product-security/bulletins/august-2021-bulletin	O-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 **CVE ID : CVE-2021-1916**	https://www.qualcomm.com/company/product-security/bulletins/august-2021-bulletin	O-QUA-QCA6-200921/2784
Integer Underflow (Wrap or Wraparound)	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.com/company/product-security/bulletins/august-2021-bulletin	O-QUA-QCA6-200921/2785
Integer Underflow (Wrap or Wraparound)	08-Sep-21	10	Integer underflow can occur 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.com/company/product-security/bulletins/august-2021-bulletin	O-QUA-QCA6-200921/2786

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.com/company/product-security/bulletins/august-2021-bulletin	O-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.com/company/product-security/bulletins/august-2021-bulletin	O-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.com/company/product-security/bulletins/august-2021-bulletin	O-QUA-QCA6-200921/2789
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.com/company/product-security/bull	O-QUA-QCA6-200921/2790

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_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.com/company/product-security/bulletins/august-2021-bulletin	O-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.com/company/product-security/bulletins/august-2021-bulletin	O-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 **CVE ID : CVE-2021-1916**	https://www.qualcomm.com/company/product-security/bulletins/august-2021-bulletin	O-QUA-QCA6-200921/2793
Integer Underflow (Wrap or Wraparound)	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.com/company/product-security/bulletins/august-2021-bulletin	O-QUA-QCA6-200921/2794
Integer Underflow (Wrap or Wraparound)	08-Sep-21	10	Integer underflow can occur due to improper 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.com/company/product-security/bulletins/august-2021-bulletin	O-QUA-QCA6-200921/2795
Incorrect	08-Sep-21	4.6	Incorrect pointer argument	https://www.	O-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.com/company/product-security/bulletins/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.com/company/product-security/bulletins/august-2021-bulletin	O-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.com/company/product-security/bulletins/august-2021-bulletin	O-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.com/company/product-security/bulletins/august-2021-bulletin	O-QUA-QCA6-200921/2799

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**		
qca6438_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.com/company/product-security/bulletins/august-2021-bulletin	O-QUA-QCA6-200921/2800
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	08-Sep-21	10	Possible buffer overflow due to 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 Networking **CVE ID : CVE-2021-1972**	https://www.qualcomm.com/company/product-security/bulletins/august-2021-bulletin	O-QUA-QCA6-200921/2801
qca6564au_firmware					
Exposure of Resource to	08-Sep-21	2.1	Child process can leak information from parent	https://www.qualcomm.co	O-QUA-QCA6-

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/bulletins/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.com/company/product-security/bulletins/august-2021-bulletin	O-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.com/company/product-security/bulletins/august-2021-bulletin	O-QUA-QCA6-200921/2804

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Integer Underflow (Wrap or Wraparound)	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.com/company/product-security/bulletins/august-2021-bulletin	O-QUA-QCA6-200921/2805
Integer Underflow (Wrap or Wraparound)	08-Sep-21	10	Integer underflow can occur due to improper 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.com/company/product-security/bulletins/august-2021-bulletin	O-QUA-QCA6-200921/2806
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.com/company/product-security/bulletins/august-2021-bulletin	O-QUA-QCA6-200921/2807
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.com/company/	O-QUA-QCA6-200921/2808

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 **CVE ID : CVE-2021-1930**	product-security/bulletins/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 Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1972**	https://www.qualcomm.com/company/product-security/bulletins/august-2021-bulletin	O-QUA-QCA6-200921/2809
qca6564a_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.com/company/product-security/bulletins/august-2021-bulletin	O-QUA-QCA6-200921/2810
Loop with	08-Sep-21	5	Loop with unreachable exit	https://www.	O-QUA-QCA6-

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.com/company/product-security/bulletins/august-2021-bulletin	200921/2811
Out-of-bounds Write	08-Sep-21	10	Possible buffer underflow due to lack of check for negative indices values when 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.com/company/product-security/bulletins/august-2021-bulletin	O-QUA-QCA6-200921/2812
Integer Underflow (Wrap or Wraparound)	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.com/company/product-security/bulletins/august-2021-bulletin	O-QUA-QCA6-200921/2813
Integer	08-Sep-21	10	Integer underflow can occur	https://www.	O-QUA-QCA6-

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Underflow (Wrap or Wraparound)			due to improper 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.com/company/product-security/bulletins/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.com/company/product-security/bulletins/august-2021-bulletin	O-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 Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1972**	https://www.qualcomm.com/company/product-security/bulletins/august-2021-bulletin	O-QUA-QCA6-200921/2816
qca6564_firmware					

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.com/company/product-security/bulletins/august-2021-bulletin	O-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 Mobile, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1972**	https://www.qualcomm.com/company/product-security/bulletins/august-2021-bulletin	O-QUA-QCA6-200921/2818
qca6574au_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,	https://www.qualcomm.com/company/product-security/bulletins/august-2021-bulletin	O-QUA-QCA6-200921/2819

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 **CVE ID : CVE-2021-1914**	https://www.qualcomm.com/company/product-security/bulletins/august-2021-bulletin	O-QUA-QCA6-200921/2820
Out-of-bounds Write	08-Sep-21	10	Possible buffer underflow due to lack of check for negative indices values when 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.com/company/product-security/bulletins/august-2021-bulletin	O-QUA-QCA6-200921/2821
Integer Underflow (Wrap or Wraparound)	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.com/company/product-security/bulletins/august-2021-bulletin	O-QUA-QCA6-200921/2822

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 Wraparound)	08-Sep-21	10	Integer underflow can occur due to improper 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.com/company/product-security/bulletins/august-2021-bulletin	O-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.com/company/product-security/bulletins/august-2021-bulletin	O-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.com/company/product-security/bulletins/august-2021-bulletin	O-QUA-QCA6-200921/2825

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.com/company/product-security/bulletins/august-2021-bulletin	O-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 Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1972**	https://www.qualcomm.com/company/product-security/bulletins/august-2021-bulletin	O-QUA-QCA6-200921/2827
qca6574a_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,	https://www.qualcomm.com/company/product-security/bulletins/august-2021-bulletin	O-QUA-QCA6-200921/2828

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.com/company/product-security/bulletins/august-2021-bulletin	O-QUA-QCA6-200921/2829
Out-of-bounds Write	08-Sep-21	10	Possible buffer underflow due to lack of check for negative indices values when 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.com/company/product-security/bulletins/august-2021-bulletin	O-QUA-QCA6-200921/2830
Integer Underflow (Wrap or Wraparound)	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.com/company/product-security/bulletins/august-2021-bulletin	O-QUA-QCA6-200921/2831

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Wearables **CVE ID : CVE-2021-1919**		
Integer Underflow (Wrap or Wraparound)	08-Sep-21	10	Integer underflow can occur due to improper 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.com/company/product-security/bulletins/august-2021-bulletin	O-QUA-QCA6-200921/2832
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.com/company/product-security/bulletins/august-2021-bulletin	O-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.com/company/product-security/bulletins/august-2021-bulletin	O-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.com/company/product-	O-QUA-QCA6-200921/2835

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 **CVE ID : CVE-2021-1930**	security/bulletins/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 Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1972**	https://www.qualcomm.com/company/product-security/bulletins/august-2021-bulletin	O-QUA-QCA6-200921/2836
qca6574_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.com/company/product-security/bulletins/august-2021-bulletin	O-QUA-QCA6-200921/2837
Loop with Unreachable	08-Sep-21	5	Loop with unreachable exit condition may occur due to	https://www.qualcomm.co	O-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/bulletins/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.com/company/product-security/bulletins/august-2021-bulletin	O-QUA-QCA6-200921/2839
Integer Underflow (Wrap or Wraparound)	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.com/company/product-security/bulletins/august-2021-bulletin	O-QUA-QCA6-200921/2840
Integer Underflow	08-Sep-21	10	Integer underflow can occur due to improper handling of	https://www.qualcomm.co	O-QUA-QCA6-200921/2841

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
(Wrap or Wraparound)			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/bulletins/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.com/company/product-security/bulletins/august-2021-bulletin	O-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.com/company/product-security/bulletins/august-2021-bulletin	O-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.com/company/product-security/bulletins/august-2021-bulletin	O-QUA-QCA6-200921/2844

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_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.com/company/product-security/bulletins/august-2021-bulletin	O-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.com/company/product-security/bulletins/august-2021-bulletin	O-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.com/company/product-	O-QUA-QCA6-200921/2847

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/bulletins/august-2021-bulletin	
Integer Underflow (Wrap or Wraparound)	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.com/company/product-security/bulletins/august-2021-bulletin	O-QUA-QCA6-200921/2848
Integer Underflow (Wrap or Wraparound)	08-Sep-21	10	Integer underflow can occur due to improper 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.com/company/product-security/bulletins/august-2021-bulletin	O-QUA-QCA6-200921/2849
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.com/company/product-security/bull	O-QUA-QCA6-200921/2850

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 **CVE ID : CVE-2021-1930**	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 Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1972**	https://www.qualcomm.com/company/product-security/bulletins/august-2021-bulletin	O-QUA-QCA6-200921/2851
qca6584_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.com/company/product-security/bulletins/august-2021-bulletin	O-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.com/company/	O-QUA-QCA6-200921/2853

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/bulletins/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.com/company/product-security/bulletins/august-2021-bulletin	O-QUA-QCA6-200921/2854
Integer Underflow (Wrap or Wraparound)	08-Sep-21	10	Integer underflow can occur due to improper 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.com/company/product-security/bulletins/august-2021-bulletin	O-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.com/company/	O-QUA-QCA6-200921/2856

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/bulletins/august-2021-bulletin	
qca6595au_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.com/company/product-security/bulletins/august-2021-bulletin	O-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.com/company/product-security/bulletins/august-2021-bulletin	O-QUA-QCA6-200921/2858

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 **CVE ID : CVE-2021-1916**	https://www.qualcomm.com/company/product-security/bulletins/august-2021-bulletin	O-QUA-QCA6-200921/2859
Integer Underflow (Wrap or Wraparound)	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.com/company/product-security/bulletins/august-2021-bulletin	O-QUA-QCA6-200921/2860
Integer Underflow (Wrap or Wraparound)	08-Sep-21	10	Integer underflow can occur due to improper 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.com/company/product-security/bulletins/august-2021-bulletin	O-QUA-QCA6-200921/2861

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.com/company/product-security/bulletins/august-2021-bulletin	O-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.com/company/product-security/bulletins/august-2021-bulletin	O-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.com/company/product-security/bulletins/august-2021-bulletin	O-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.com/company/product-security/bulletins/august-2021-bulletin	O-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_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.com/company/product-security/bulletins/august-2021-bulletin	O-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.com/company/product-security/bulletins/august-2021-bulletin	O-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.com/company/product-security/bulletins/august-	O-QUA-QCA6-200921/2868

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wearables **CVE ID : CVE-2021-1929**	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 Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1972**	https://www.qualcomm.com/company/product-security/bulletins/august-2021-bulletin	O-QUA-QCA6-200921/2869
qca6694au_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.com/company/product-security/bulletins/august-2021-bulletin	O-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.com/company/product-	O-QUA-QCA6-200921/2871

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/bulletins/august-2021-bulletin	
Integer Underflow (Wrap or Wraparound)	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.com/company/product-security/bulletins/august-2021-bulletin	O-QUA-QCA6-200921/2872
Integer Underflow (Wrap or Wraparound)	08-Sep-21	10	Integer underflow can occur due to improper 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.com/company/product-security/bulletins/august-2021-bulletin	O-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.com/company/product-	O-QUA-QCA6-200921/2874

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/bulletins/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.com/company/product-security/bulletins/august-2021-bulletin	O-QUA-QCA6-200921/2875
Integer Underflow (Wrap or Wraparound)	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.com/company/product-security/bulletins/august-2021-bulletin	O-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.com/company/product-	O-QUA-QCA6-200921/2877

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/bulletins/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.com/company/product-security/bulletins/august-2021-bulletin	O-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 Mobile, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1972**	https://www.qualcomm.com/company/product-security/bulletins/august-2021-bulletin	O-QUA-QCA6-200921/2879
qca6696_firmware					
Exposure of	08-Sep-21	2.1	Child process can leak	https://www.	O-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 Voice & Music, Snapdragon Wearables **CVE ID : CVE-2021-1904**	qualcomm.com/company/product-security/bulletins/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.com/company/product-security/bulletins/august-2021-bulletin	O-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.com/company/product-security/bulletins/august-2021-bulletin	O-QUA-QCA6-200921/2882

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2021-1916		
Integer Underflow (Wrap or Wraparound)	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.com/company/product-security/bulletins/august-2021-bulletin	O-QUA-QCA6-200921/2883
Integer Underflow (Wrap or Wraparound)	08-Sep-21	10	Integer underflow can occur due to improper 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.com/company/product-security/bulletins/august-2021-bulletin	O-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.com/company/product-security/bulletins/august-2021-bulletin	O-QUA-QCA6-200921/2885
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.com/company/product-	O-QUA-QCA6-200921/2886

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/bulletins/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.com/company/product-security/bulletins/august-2021-bulletin	O-QUA-QCA6-200921/2887
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	08-Sep-21	10	Possible buffer overflow due to 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 Networking **CVE ID : CVE-2021-1972**	https://www.qualcomm.com/company/product-security/bulletins/august-2021-bulletin	O-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.com/company/product-security/bull	O-QUA-QCA7-200921/2889

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 Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1972**	https://www.qualcomm.com/company/product-security/bulletins/august-2021-bulletin	O-QUA-QCA7-200921/2890
qca7520_firmware					
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	08-Sep-21	10	Possible buffer overflow due to 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 Networking	https://www.qualcomm.com/company/product-security/bulletins/august-2021-bulletin	O-QUA-QCA7-200921/2891

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2021-1972		
qca7550_firmware					
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	08-Sep-21	10	Possible buffer overflow due to 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 Networking **CVE ID : CVE-2021-1972**	https://www.qualcomm.com/company/product-security/bulletins/august-2021-bulletin	O-QUA-QCA7-200921/2892
qca8072_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.com/company/product-security/bulletins/august-2021-bulletin	O-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.com/company/product-security/bulletins/august-2021-bulletin	O-QUA-QCA8-200921/2894

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_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.com/company/product-security/bulletins/august-2021-bulletin	O-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 Mobile, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1972**	https://www.qualcomm.com/company/product-security/bulletins/august-2021-bulletin	O-QUA-QCA8-200921/2896
qca8081_firmware					

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.com/company/product-security/bulletins/august-2021-bulletin	O-QUA-QCA8-200921/2897
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	08-Sep-21	10	Possible buffer overflow due to 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 Networking **CVE ID : CVE-2021-1972**	https://www.qualcomm.com/company/product-security/bulletins/august-2021-bulletin	O-QUA-QCA8-200921/2898
qca8337_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,	https://www.qualcomm.com/company/product-security/bulletins/august-2021-bulletin	O-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 Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1972**	https://www.qualcomm.com/company/product-security/bulletins/august-2021-bulletin	O-QUA-QCA8-200921/2900
qca9367_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.com/company/product-security/bulletins/august-2021-bulletin	O-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.com/company/product-	O-QUA-QCA9-200921/2902

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/bulletins/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.com/company/product-security/bulletins/august-2021-bulletin	O-QUA-QCA9-200921/2903
Integer Underflow (Wrap or Wraparound)	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.com/company/product-security/bulletins/august-2021-bulletin	O-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.com/company/product-	O-QUA-QCA9-200921/2905

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/bulletins/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.com/company/product-security/bulletins/august-2021-bulletin	O-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 Mobile, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1972**	https://www.qualcomm.com/company/product-security/bulletins/august-2021-bulletin	O-QUA-QCA9-200921/2907
qca9377_firmware					
Exposure of	08-Sep-21	2.1	Child process can leak	https://www.	O-QUA-QCA9-

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 Voice & Music, Snapdragon Wearables **CVE ID : CVE-2021-1904**	qualcomm.com/company/product-security/bulletins/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.com/company/product-security/bulletins/august-2021-bulletin	O-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.com/company/product-security/bulletins/august-2021-bulletin	O-QUA-QCA9-200921/2910

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2021-1916		
Integer Underflow (Wrap or Wraparound)	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.com/company/product-security/bulletins/august-2021-bulletin	O-QUA-QCA9-200921/2911
Integer Underflow (Wrap or Wraparound)	08-Sep-21	10	Integer underflow can occur due to improper 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.com/company/product-security/bulletins/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.com/company/product-security/bulletins/august-2021-bulletin	O-QUA-QCA9-200921/2913

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.com/company/product-security/bulletins/august-2021-bulletin	O-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 Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1972**	https://www.qualcomm.com/company/product-security/bulletins/august-2021-bulletin	O-QUA-QCA9-200921/2915
qca9379_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,	https://www.qualcomm.com/company/product-security/bulletins/august-2021-bulletin	O-QUA-QCA9-200921/2916

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.com/company/product-security/bulletins/august-2021-bulletin	O-QUA-QCA9-200921/2917
Out-of-bounds Write	08-Sep-21	10	Possible buffer underflow due to lack of check for negative indices values when 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.com/company/product-security/bulletins/august-2021-bulletin	O-QUA-QCA9-200921/2918
Integer Underflow (Wrap or Wraparound)	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.com/company/product-security/bulletins/august-2021-bulletin	O-QUA-QCA9-200921/2919

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Wearables **CVE ID : CVE-2021-1919**		
Integer Underflow (Wrap or Wraparound)	08-Sep-21	10	Integer underflow can occur due to improper 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.com/company/product-security/bulletins/august-2021-bulletin	O-QUA-QCA9-200921/2920
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	08-Sep-21	10	Possible buffer overflow due to 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 Networking **CVE ID : CVE-2021-1972**	https://www.qualcomm.com/company/product-security/bulletins/august-2021-bulletin	O-QUA-QCA9-200921/2921
qca9531_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 &	https://www.qualcomm.com/company/product-security/bulletins/august-2021-bulletin	O-QUA-QCA9-200921/2922

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 Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1972**	https://www.qualcomm.com/company/product-security/bulletins/august-2021-bulletin	O-QUA-QCA9-200921/2923
qca9558_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.com/company/product-security/bulletins/august-2021-bulletin	O-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.com/company/product-	O-QUA-QCA9-200921/2925

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/bulletins/august-2021-bulletin	
qca9561_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.com/company/product-security/bulletins/august-2021-bulletin	O-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 Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and	https://www.qualcomm.com/company/product-security/bulletins/august-2021-bulletin	O-QUA-QCA9-200921/2927

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Networking **CVE ID : CVE-2021-1972**		
qca9563_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.com/company/product-security/bulletins/august-2021-bulletin	O-QUA-QCA9-200921/2928
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	08-Sep-21	10	Possible buffer overflow due to 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 Networking **CVE ID : CVE-2021-1972**	https://www.qualcomm.com/company/product-security/bulletins/august-2021-bulletin	O-QUA-QCA9-200921/2929
qca9880_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	https://www.qualcomm.com/company/product-security/bulletins/august-	O-QUA-QCA9-200921/2930

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1928**	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 Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1972**	https://www.qualcomm.com/company/product-security/bulletins/august-2021-bulletin	O-QUA-QCA9-200921/2931
qca9882_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.com/company/product-security/bulletins/august-2021-bulletin	O-QUA-QCA9-200921/2932
Buffer Copy without	08-Sep-21	10	Possible buffer overflow due to improper validation of	https://www.qualcomm.co	O-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 Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1972**	m/company/product-security/bulletins/august-2021-bulletin	
qca9886_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.com/company/product-security/bulletins/august-2021-bulletin	O-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 Voice & Music, Snapdragon Wearables, Snapdragon Wired	https://www.qualcomm.com/company/product-security/bulletins/august-2021-bulletin	O-QUA-QCA9-200921/2935

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Infrastructure and Networking **CVE ID : CVE-2021-1972**		
qca9887_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.com/company/product-security/bulletins/august-2021-bulletin	O-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 Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1972**	https://www.qualcomm.com/company/product-security/bulletins/august-2021-bulletin	O-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.com/company/product-security/bull	O-QUA-QCA9-200921/2938

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 Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1972**	https://www.qualcomm.com/company/product-security/bulletins/august-2021-bulletin	O-QUA-QCA9-200921/2939
qca9889_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.com/company/product-security/bulletins/august-2021-bulletin	O-QUA-QCA9-200921/2940
Buffer Copy	08-Sep-21	10	Possible buffer overflow due	https://www.	O-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 Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1972**	qualcomm.com/company/product-security/bulletins/august-2021-bulletin	200921/2941
qca9896_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.com/company/product-security/bulletins/august-2021-bulletin	O-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.com/company/product-security/bulletins/august-2021-bulletin	O-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_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.com/company/product-security/bulletins/august-2021-bulletin	O-QUA-QCA9-200921/2944
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	08-Sep-21	10	Possible buffer overflow due to 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 Networking **CVE ID : CVE-2021-1972**	https://www.qualcomm.com/company/product-security/bulletins/august-2021-bulletin	O-QUA-QCA9-200921/2945
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.com/company/product-	O-QUA-QCA9-200921/2946

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/bulletins/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 Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1972**	https://www.qualcomm.com/company/product-security/bulletins/august-2021-bulletin	O-QUA-QCA9-200921/2947
qca9982_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.com/company/product-security/bulletins/august-2021-bulletin	O-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 Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1972**	https://www.qualcomm.com/company/product-security/bulletins/august-2021-bulletin	O-QUA-QCA9-200921/2949
qca9984_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.com/company/product-security/bulletins/august-2021-bulletin	O-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.com/company/product-security/bulletins/august-2021-bulletin	O-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_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.com/company/product-security/bulletins/august-2021-bulletin	O-QUA-QCA9-200921/2952
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	08-Sep-21	10	Possible buffer overflow due to 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 Networking **CVE ID : CVE-2021-1972**	https://www.qualcomm.com/company/product-security/bulletins/august-2021-bulletin	O-QUA-QCA9-200921/2953
qca9986_firmware					
Buffer Copy without Checking	08-Sep-21	10	Possible buffer overflow due to improper validation of device types during P2P	https://www.qualcomm.com/company/	O-QUA-QCA9-200921/2954

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/bulletins/august-2021-bulletin	
qca9987_firmware					
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	08-Sep-21	10	Possible buffer overflow due to 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 Networking **CVE ID : CVE-2021-1972**	https://www.qualcomm.com/company/product-security/bulletins/august-2021-bulletin	O-QUA-QCA9-200921/2955
qca9988_firmware					
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	08-Sep-21	10	Possible buffer overflow due 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.com/company/product-security/bulletins/august-2021-bulletin	O-QUA-QCA9-200921/2956

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_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.com/company/product-security/bulletins/august-2021-bulletin	O-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 Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1972**	https://www.qualcomm.com/company/product-security/bulletins/august-2021-bulletin	O-QUA-QCA9-200921/2958
qca9992_firmware					
Out-of-bounds	08-Sep-21	3.6	Buffer over read could occur due to incorrect check of	https://www.qualcomm.co	O-QUA-QCA9-

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/bulletins/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 Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1972**	https://www.qualcomm.com/company/product-security/bulletins/august-2021-bulletin	O-QUA-QCA9-200921/2960
qca9994_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	https://www.qualcomm.com/company/product-security/bulletins/august-2021-bulletin	O-QUA-QCA9-200921/2961

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 Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1972**	https://www.qualcomm.com/company/product-security/bulletins/august-2021-bulletin	O-QUA-QCA9-200921/2962
qcm2290_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.com/company/product-security/bulletins/august-2021-bulletin	O-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.com/company/product-security/bulletins/august-	O-QUA-QCM2-200921/2964

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.com/company/product-security/bulletins/august-2021-bulletin	O-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.com/company/product-security/bulletins/august-2021-bulletin	O-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 Mobile, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking	https://www.qualcomm.com/company/product-security/bulletins/august-2021-bulletin	O-QUA-QCM2-200921/2967

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2021-1972		
qcm4290_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.com/company/product-security/bulletins/august-2021-bulletin	O-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.com/company/product-security/bulletins/august-2021-bulletin	O-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.com/company/product-security/bulletins/august-2021-bulletin	O-QUA-QCM4-200921/2970

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 Wraparound)	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.com/company/product-security/bulletins/august-2021-bulletin	O-QUA-QCM4-200921/2971
Integer Underflow (Wrap or Wraparound)	08-Sep-21	10	Integer underflow can occur due to improper 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.com/company/product-security/bulletins/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.com/company/product-security/bulletins/august-2021-bulletin	O-QUA-QCM4-200921/2973

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.com/company/product-security/bulletins/august-2021-bulletin	O-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.com/company/product-security/bulletins/august-2021-bulletin	O-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 Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1972**	https://www.qualcomm.com/company/product-security/bulletins/august-2021-bulletin	O-QUA-QCM4-200921/2976
qcm6125_firmware					
Exposure of	08-Sep-21	2.1	Child process can leak	https://www.	O-QUA-QCM6-

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 Voice & Music, Snapdragon Wearables **CVE ID : CVE-2021-1904**	qualcomm.com/company/product-security/bulletins/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.com/company/product-security/bulletins/august-2021-bulletin	O-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.com/company/product-security/bulletins/august-2021-bulletin	O-QUA-QCM6-200921/2979

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2021-1916		
Integer Underflow (Wrap or Wraparound)	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.com/company/product-security/bulletins/august-2021-bulletin	O-QUA-QCM6-200921/2980
Integer Underflow (Wrap or Wraparound)	08-Sep-21	10	Integer underflow can occur due to improper 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.com/company/product-security/bulletins/august-2021-bulletin	O-QUA-QCM6-200921/2981
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.com/company/product-security/bulletins/august-2021-bulletin	O-QUA-QCM6-200921/2982
Improper Restriction	08-Sep-21	3.6	Possible out of bounds read due to incorrect validation of	https://www.qualcomm.co	O-QUA-QCM6-200921/2983

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/bulletins/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 Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1972**	https://www.qualcomm.com/company/product-security/bulletins/august-2021-bulletin	O-QUA-QCM6-200921/2984
qcn3018_firmware					
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	08-Sep-21	10	Possible buffer overflow due to 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 Networking	https://www.qualcomm.com/company/product-security/bulletins/august-2021-bulletin	O-QUA-QCN3-200921/2985

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 **CVE ID : CVE-2021-1928**	https://www.qualcomm.com/company/product-security/bulletins/august-2021-bulletin	O-QUA-QCN5-200921/2986
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	08-Sep-21	10	Possible buffer overflow due to 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 Networking **CVE ID : CVE-2021-1972**	https://www.qualcomm.com/company/product-security/bulletins/august-2021-bulletin	O-QUA-QCN5-200921/2987
qcn5022_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	https://www.qualcomm.com/company/product-security/bulletins/august-2021-bulletin	O-QUA-QCN5-200921/2988

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 Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1972**	https://www.qualcomm.com/company/product-security/bulletins/august-2021-bulletin	O-QUA-QCN5-200921/2989
qcn5024_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.com/company/product-security/bulletins/august-2021-bulletin	O-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.com/company/	O-QUA-QCN5-200921/2991

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/bulletins/august-2021-bulletin	
qcn5052_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.com/company/product-security/bulletins/august-2021-bulletin	O-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 Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and	https://www.qualcomm.com/company/product-security/bulletins/august-2021-bulletin	O-QUA-QCN5-200921/2993

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Networking **CVE ID : CVE-2021-1972**		
qcn5054_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.com/company/product-security/bulletins/august-2021-bulletin	O-QUA-QCN5-200921/2994
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	08-Sep-21	10	Possible buffer overflow due to 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 Networking **CVE ID : CVE-2021-1972**	https://www.qualcomm.com/company/product-security/bulletins/august-2021-bulletin	O-QUA-QCN5-200921/2995
qcn5064_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	https://www.qualcomm.com/company/product-security/bulletins/august-	O-QUA-QCN5-200921/2996

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1928**	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 Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1972**	https://www.qualcomm.com/company/product-security/bulletins/august-2021-bulletin	O-QUA-QCN5-200921/2997
qcn5121_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.com/company/product-security/bulletins/august-2021-bulletin	O-QUA-QCN5-200921/2998
Buffer Copy without	08-Sep-21	10	Possible buffer overflow due to improper validation of	https://www.qualcomm.co	O-QUA-QCN5-200921/2999

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 Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1972**	m/company/product-security/bulletins/august-2021-bulletin	
qcn5122_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.com/company/product-security/bulletins/august-2021-bulletin	O-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 Voice & Music, Snapdragon Wearables, Snapdragon Wired	https://www.qualcomm.com/company/product-security/bulletins/august-2021-bulletin	O-QUA-QCN5-200921/3001

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Infrastructure and Networking **CVE ID : CVE-2021-1972**		
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.com/company/product-security/bulletins/august-2021-bulletin	O-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 Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1972**	https://www.qualcomm.com/company/product-security/bulletins/august-2021-bulletin	O-QUA-QCN5-200921/3003
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.com/company/product-security/bull	O-QUA-QCN5-200921/3004

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 Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1972**	https://www.qualcomm.com/company/product-security/bulletins/august-2021-bulletin	O-QUA-QCN5-200921/3005
qcn5154_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.com/company/product-security/bulletins/august-2021-bulletin	O-QUA-QCN5-200921/3006
Buffer Copy	08-Sep-21	10	Possible buffer overflow due	https://www.	O-QUA-QCN5-

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 Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1972**	qualcomm.com/company/product-security/bulletins/august-2021-bulletin	200921/3007
qcn5164_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.com/company/product-security/bulletins/august-2021-bulletin	O-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.com/company/product-security/bulletins/august-2021-bulletin	O-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_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.com/company/product-security/bulletins/august-2021-bulletin	O-QUA-QCN5-200921/3010
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	08-Sep-21	10	Possible buffer overflow due to 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 Networking **CVE ID : CVE-2021-1972**	https://www.qualcomm.com/company/product-security/bulletins/august-2021-bulletin	O-QUA-QCN5-200921/3011
qcn5502_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.com/company/product-	O-QUA-QCN5-200921/3012

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/bulletins/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 Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1972**	https://www.qualcomm.com/company/product-security/bulletins/august-2021-bulletin	O-QUA-QCN5-200921/3013
qcn5550_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.com/company/product-security/bulletins/august-2021-bulletin	O-QUA-QCN5-200921/3014

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 Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1972**	https://www.qualcomm.com/company/product-security/bulletins/august-2021-bulletin	O-QUA-QCN5-200921/3015
qcn6023_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.com/company/product-security/bulletins/august-2021-bulletin	O-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.com/company/product-security/bulletins/august-2021-bulletin	O-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_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.com/company/product-security/bulletins/august-2021-bulletin	O-QUA-QCN6-200921/3018
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	08-Sep-21	10	Possible buffer overflow due to 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 Networking **CVE ID : CVE-2021-1972**	https://www.qualcomm.com/company/product-security/bulletins/august-2021-bulletin	O-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.com/company/	O-QUA-QCN6-200921/3020

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/bulletins/august-2021-bulletin	
qcn9000_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.com/company/product-security/bulletins/august-2021-bulletin	O-QUA-QCN9-200921/3021
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	08-Sep-21	10	Possible buffer overflow due to 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	https://www.qualcomm.com/company/product-security/bulletins/august-2021-bulletin	O-QUA-QCN9-200921/3022

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Networking **CVE ID : CVE-2021-1972**		
qcn9012_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.com/company/product-security/bulletins/august-2021-bulletin	O-QUA-QCN9-200921/3023
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	08-Sep-21	10	Possible buffer overflow due to 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 Networking **CVE ID : CVE-2021-1972**	https://www.qualcomm.com/company/product-security/bulletins/august-2021-bulletin	O-QUA-QCN9-200921/3024
qcn9022_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	https://www.qualcomm.com/company/product-security/bulletins/august-	O-QUA-QCN9-200921/3025

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1928**	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 Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1972**	https://www.qualcomm.com/company/product-security/bulletins/august-2021-bulletin	O-QUA-QCN9-200921/3026
qcn9024_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.com/company/product-security/bulletins/august-2021-bulletin	O-QUA-QCN9-200921/3027
Buffer Copy without	08-Sep-21	10	Possible buffer overflow due to improper validation of	https://www.qualcomm.co	O-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 Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1972**	m/company/product-security/bulletins/august-2021-bulletin	
qcn9070_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.com/company/product-security/bulletins/august-2021-bulletin	O-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 Voice & Music, Snapdragon Wearables, Snapdragon Wired	https://www.qualcomm.com/company/product-security/bulletins/august-2021-bulletin	O-QUA-QCN9-200921/3030

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Infrastructure and Networking **CVE ID : CVE-2021-1972**		
qcn9072_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.com/company/product-security/bulletins/august-2021-bulletin	O-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 Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1972**	https://www.qualcomm.com/company/product-security/bulletins/august-2021-bulletin	O-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.com/company/product-security/bull	O-QUA-QCN9-200921/3033

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 Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1972**	https://www.qualcomm.com/company/product-security/bulletins/august-2021-bulletin	O-QUA-QCN9-200921/3034
qcn9100_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.com/company/product-security/bulletins/august-2021-bulletin	O-QUA-QCN9-200921/3035
Buffer Copy	08-Sep-21	10	Possible buffer overflow due	https://www.	O-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 Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1972**	qualcomm.com/company/product-security/bulletins/august-2021-bulletin	200921/3036
qcs2290_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.com/company/product-security/bulletins/august-2021-bulletin	O-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.com/company/product-security/bulletins/august-2021-bulletin	O-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.com/company/product-security/bulletins/august-2021-bulletin	O-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.com/company/product-security/bulletins/august-2021-bulletin	O-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 Mobile, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1972**	https://www.qualcomm.com/company/product-security/bulletins/august-2021-bulletin	O-QUA-QCS2-200921/3041
qcs405_firmware					
Exposure of	08-Sep-21	2.1	Child process can leak	https://www.	O-QUA-QCS4-

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 Voice & Music, Snapdragon Wearables **CVE ID : CVE-2021-1904**	qualcomm.com/company/product-security/bulletins/august-2021-bulletin	200921/3042
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	08-Sep-21	10	Possible buffer overflow due to 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 Networking **CVE ID : CVE-2021-1972**	https://www.qualcomm.com/company/product-security/bulletins/august-2021-bulletin	O-QUA-QCS4-200921/3043
qcs410_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,	https://www.qualcomm.com/company/product-security/bulletins/august-2021-bulletin	O-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.com/company/product-security/bulletins/august-2021-bulletin	O-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.com/company/product-security/bulletins/august-2021-bulletin	O-QUA-QCS4-200921/3046
Integer Underflow (Wrap or Wraparound)	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.com/company/product-security/bulletins/august-2021-bulletin	O-QUA-QCS4-200921/3047

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 Wraparound)	08-Sep-21	10	Integer underflow can occur due to improper 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.com/company/product-security/bulletins/august-2021-bulletin	O-QUA-QCS4-200921/3048
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.com/company/product-security/bulletins/august-2021-bulletin	O-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 Voice & Music, Snapdragon Wearables, Snapdragon Wired	https://www.qualcomm.com/company/product-security/bulletins/august-2021-bulletin	O-QUA-QCS4-200921/3050

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Infrastructure and Networking **CVE ID : CVE-2021-1972**		
qcs4290_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.com/company/product-security/bulletins/august-2021-bulletin	O-QUA-QCS4-200921/3051
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.com/company/product-security/bulletins/august-2021-bulletin	O-QUA-QCS4-200921/3052
Out-of-bounds Write	08-Sep-21	10	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.com/company/product-security/bulletins/august-2021-bulletin	O-QUA-QCS4-200921/3053

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 Wraparound)	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.com/company/product-security/bulletins/august-2021-bulletin	O-QUA-QCS4-200921/3054
Integer Underflow (Wrap or Wraparound)	08-Sep-21	10	Integer underflow can occur due to improper 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.com/company/product-security/bulletins/august-2021-bulletin	O-QUA-QCS4-200921/3055
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.com/company/product-security/bulletins/august-2021-bulletin	O-QUA-QCS4-200921/3056

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.com/company/product-security/bulletins/august-2021-bulletin	O-QUA-QCS4-200921/3057
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.com/company/product-security/bulletins/august-2021-bulletin	O-QUA-QCS4-200921/3058
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	08-Sep-21	10	Possible buffer overflow due to 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 Networking **CVE ID : CVE-2021-1972**	https://www.qualcomm.com/company/product-security/bulletins/august-2021-bulletin	O-QUA-QCS4-200921/3059
qcs603_firmware					

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.com/company/product-security/bulletins/august-2021-bulletin	O-QUA-QCS6-200921/3060
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.com/company/product-security/bulletins/august-2021-bulletin	O-QUA-QCS6-200921/3061
Out-of-bounds Write	08-Sep-21	10	Possible buffer underflow due to lack of check for negative indices values when 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.com/company/product-security/bulletins/august-2021-bulletin	O-QUA-QCS6-200921/3062

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2021-1916		
Integer Underflow (Wrap or Wraparound)	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.com/company/product-security/bulletins/august-2021-bulletin	O-QUA-QCS6-200921/3063
Integer Underflow (Wrap or Wraparound)	08-Sep-21	10	Integer underflow can occur due to improper 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.com/company/product-security/bulletins/august-2021-bulletin	O-QUA-QCS6-200921/3064
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.com/company/product-security/bulletins/august-2021-bulletin	O-QUA-QCS6-200921/3065
Buffer Copy without	08-Sep-21	10	Possible buffer overflow due to improper validation of	https://www.qualcomm.co	O-QUA-QCS6-200921/3066

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 Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1972**	m/company/product-security/bulletins/august-2021-bulletin	
qcs605_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.com/company/product-security/bulletins/august-2021-bulletin	O-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.com/company/product-security/bulletins/august-2021-bulletin	O-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 **CVE ID : CVE-2021-1916**	https://www.qualcomm.com/company/product-security/bulletins/august-2021-bulletin	O-QUA-QCS6-200921/3069
Integer Underflow (Wrap or Wraparound)	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.com/company/product-security/bulletins/august-2021-bulletin	O-QUA-QCS6-200921/3070
Integer Underflow (Wrap or Wraparound)	08-Sep-21	10	Integer underflow can occur due to improper 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.com/company/product-security/bulletins/august-2021-bulletin	O-QUA-QCS6-200921/3071

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.com/company/product-security/bulletins/august-2021-bulletin	O-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 Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1972**	https://www.qualcomm.com/company/product-security/bulletins/august-2021-bulletin	O-QUA-QCS6-200921/3073
qcs610_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,	https://www.qualcomm.com/company/product-security/bulletins/august-2021-bulletin	O-QUA-QCS6-200921/3074

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.com/company/product-security/bulletins/august-2021-bulletin	O-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.com/company/product-security/bulletins/august-2021-bulletin	O-QUA-QCS6-200921/3076
Integer Underflow (Wrap or Wraparound)	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.com/company/product-security/bulletins/august-2021-bulletin	O-QUA-QCS6-200921/3077

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 Wraparound)	08-Sep-21	10	Integer underflow can occur due to improper 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.com/company/product-security/bulletins/august-2021-bulletin	O-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.com/company/product-security/bulletins/august-2021-bulletin	O-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.com/company/product-security/bulletins/august-2021-bulletin	O-QUA-QCS6-200921/3080

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 Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1972**	https://www.qualcomm.com/company/product-security/bulletins/august-2021-bulletin	O-QUA-QCS6-200921/3081
qcs6125_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.com/company/product-security/bulletins/august-2021-bulletin	O-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.com/company/product-security/bulletins/august-2021-bulletin	O-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 **CVE ID : CVE-2021-1916**	https://www.qualcomm.com/company/product-security/bulletins/august-2021-bulletin	O-QUA-QCS6-200921/3084
Integer Underflow (Wrap or Wraparound)	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.com/company/product-security/bulletins/august-2021-bulletin	O-QUA-QCS6-200921/3085
Integer Underflow (Wrap or Wraparound)	08-Sep-21	10	Integer underflow can occur 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.com/company/product-security/bulletins/august-2021-bulletin	O-QUA-QCS6-200921/3086

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.com/company/product-security/bulletins/august-2021-bulletin	O-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.com/company/product-security/bulletins/august-2021-bulletin	O-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 Mobile, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking	https://www.qualcomm.com/company/product-security/bulletins/august-2021-bulletin	O-QUA-QCS6-200921/3089

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2021-1972		
qcx315_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.com/company/product-security/bulletins/august-2021-bulletin	O-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.com/company/product-security/bulletins/august-2021-bulletin	O-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.com/company/product-security/bulletins/august-2021-bulletin	O-QUA-QCX3-200921/3092

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 Wraparound)	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.com/company/product-security/bulletins/august-2021-bulletin	O-QUA-QCX3-200921/3093
Integer Underflow (Wrap or Wraparound)	08-Sep-21	10	Integer underflow can occur due to improper 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.com/company/product-security/bulletins/august-2021-bulletin	O-QUA-QCX3-200921/3094
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	08-Sep-21	10	Possible buffer overflow due to 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.com/company/product-security/bulletins/august-2021-bulletin	O-QUA-QCX3-200921/3095

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1972**		
qet4101_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.com/company/product-security/bulletins/august-2021-bulletin	O-QUA-QET4-200921/3096
qfe1922_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.com/company/product-security/bulletins/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.com/company/product-	O-QUA-QFE1-200921/3098

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/bulletins/august-2021-bulletin	
qfe1952_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.com/company/product-security/bulletins/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 Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and	https://www.qualcomm.com/company/product-security/bulletins/august-2021-bulletin	O-QUA-QFE1-200921/3100

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Networking **CVE ID : CVE-2021-1972**		
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 Voice & Music, Snapdragon Wearables **CVE ID : CVE-2021-1904**	https://www.qualcomm.com/company/product-security/bulletins/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.com/company/product-security/bulletins/august-2021-bulletin	O-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.com/company/product-security/bulletins/august-2021-bulletin	O-QUA-QRB5-200921/3103

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1972**		
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 Voice & Music, Snapdragon Wearables **CVE ID : CVE-2021-1904**	https://www.qualcomm.com/company/product-security/bulletins/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.com/company/product-security/bulletins/august-2021-bulletin	O-QUA-QSM8-200921/3105
qsm8350_firmware					
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.com/company/product-security/bulletins/august-2021-bulletin	O-QUA-QSM8-200921/3106

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.com/company/product-security/bulletins/august-2021-bulletin	O-QUA-QSM8-200921/3107
qsw8573_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.com/company/product-security/bulletins/august-2021-bulletin	O-QUA-QSW8-200921/3108
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.com/company/product-security/bulletins/august-2021-bulletin	O-QUA-QSW8-200921/3109

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 **CVE ID : CVE-2021-1916**	https://www.qualcomm.com/company/product-security/bulletins/august-2021-bulletin	O-QUA-QSW8-200921/3110
Integer Underflow (Wrap or Wraparound)	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.com/company/product-security/bulletins/august-2021-bulletin	O-QUA-QSW8-200921/3111
Integer Underflow (Wrap or Wraparound)	08-Sep-21	10	Integer underflow can occur due to improper 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.com/company/product-security/bulletins/august-2021-bulletin	O-QUA-QSW8-200921/3112

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2021-1920		
qualcomm215_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.com/company/product-security/bulletins/august-2021-bulletin	O-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.com/company/product-security/bulletins/august-2021-bulletin	O-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.com/company/product-security/bulletins/august-2021-bulletin	O-QUA-QUAL-200921/3115

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 Wraparound)	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.com/company/product-security/bulletins/august-2021-bulletin	O-QUA-QUAL-200921/3116
Integer Underflow (Wrap or Wraparound)	08-Sep-21	10	Integer underflow can occur due to improper 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.com/company/product-security/bulletins/august-2021-bulletin	O-QUA-QUAL-200921/3117
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.com/company/product-security/bulletins/august-2021-bulletin	O-QUA-QUAL-200921/3118

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.com/company/product-security/bulletins/august-2021-bulletin	O-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 Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1972**	https://www.qualcomm.com/company/product-security/bulletins/august-2021-bulletin	O-QUA-QUAL-200921/3120
sa415m_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,	https://www.qualcomm.com/company/product-security/bulletins/august-2021-bulletin	O-QUA-SA41-200921/3121

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 IoT, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2021-1914**	https://www.qualcomm.com/company/product-security/bulletins/august-2021-bulletin	O-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.com/company/product-security/bulletins/august-2021-bulletin	O-QUA-SA41-200921/3123
Integer Underflow (Wrap or Wraparound)	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.com/company/product-security/bulletins/august-	O-QUA-SA41-200921/3124

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 Wraparound)	08-Sep-21	10	Integer underflow can occur due to improper 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.com/company/product-security/bulletins/august-2021-bulletin	O-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.com/company/product-security/bulletins/august-2021-bulletin	O-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.com/company/product-security/bulletins/august-2021-bulletin	O-QUA-SA41-200921/3127

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1972**		
sa515m_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.com/company/product-security/bulletins/august-2021-bulletin	O-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.com/company/product-security/bulletins/august-2021-bulletin	O-QUA-SA51-200921/3129
Integer Underflow (Wrap or Wraparound)	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.com/company/product-security/bulletins/august-	O-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 Wraparound)	08-Sep-21	10	Integer underflow can occur due to improper 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.com/company/product-security/bulletins/august-2021-bulletin	O-QUA-SA51-200921/3131
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	08-Sep-21	10	Possible buffer overflow due to 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 Networking **CVE ID : CVE-2021-1972**	https://www.qualcomm.com/company/product-security/bulletins/august-2021-bulletin	O-QUA-SA51-200921/3132
sa6145p_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.com/company/product-	O-QUA-SA61-200921/3133

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/bulletins/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.com/company/product-security/bulletins/august-2021-bulletin	O-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.com/company/product-security/bulletins/august-2021-bulletin	O-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.com/company/product-security/bulletins/august-	O-QUA-SA61-200921/3136

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wearables **CVE ID : CVE-2021-1929**	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.com/company/product-security/bulletins/august-2021-bulletin	O-QUA-SA61-200921/3137
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	08-Sep-21	10	Possible buffer overflow due to 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 Networking **CVE ID : CVE-2021-1972**	https://www.qualcomm.com/company/product-security/bulletins/august-2021-bulletin	O-QUA-SA61-200921/3138
sa6150p_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,	https://www.qualcomm.com/company/product-security/bulletins/august-2021-bulletin	O-QUA-SA61-200921/3139

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.com/company/product-security/bulletins/august-2021-bulletin	O-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.com/company/product-security/bulletins/august-2021-bulletin	O-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.com/company/product-security/bulletins/august-2021-bulletin	O-QUA-SA61-200921/3142

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			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.com/company/product-security/bulletins/august-2021-bulletin	O-QUA-SA61-200921/3143
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	08-Sep-21	10	Possible buffer overflow due to 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 Networking **CVE ID : CVE-2021-1972**	https://www.qualcomm.com/company/product-security/bulletins/august-2021-bulletin	O-QUA-SA61-200921/3144
sa6155p_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,	https://www.qualcomm.com/company/product-security/bulletins/august-2021-bulletin	O-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 Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2021-1916**	https://www.qualcomm.com/company/product-security/bulletins/august-2021-bulletin	O-QUA-SA61-200921/3146
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.com/company/product-security/bulletins/august-2021-bulletin	O-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.com/company/product-security/bulletins/august-2021-bulletin	O-QUA-SA61-200921/3148

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.com/company/product-security/bulletins/august-2021-bulletin	O-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 Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1972**	https://www.qualcomm.com/company/product-security/bulletins/august-2021-bulletin	O-QUA-SA61-200921/3150
sa6155_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,	https://www.qualcomm.com/company/product-security/bulletins/august-2021-bulletin	O-QUA-SA61-200921/3151

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 **CVE ID : CVE-2021-1916**	https://www.qualcomm.com/company/product-security/bulletins/august-2021-bulletin	O-QUA-SA61-200921/3152
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.com/company/product-security/bulletins/august-2021-bulletin	O-QUA-SA61-200921/3153
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.com/company/product-security/bulletins/august-2021-bulletin	O-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.com/company/product-	O-QUA-SA61-200921/3155

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/bulletins/august-2021-bulletin	
sa8145p_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.com/company/product-security/bulletins/august-2021-bulletin	O-QUA-SA81-200921/3156
Out-of-bounds Write	08-Sep-21	10	Possible buffer underflow due to lack of check for negative indices values when 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.com/company/product-security/bulletins/august-2021-bulletin	O-QUA-SA81-200921/3157

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			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.com/company/product-security/bulletins/august-2021-bulletin	O-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.com/company/product-security/bulletins/august-2021-bulletin	O-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.com/company/product-security/bulletins/august-2021-bulletin	O-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.com/company/product-security/bulletins/august-2021-bulletin	O-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 **CVE ID : CVE-2021-1972**		
sa8150p_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.com/company/product-security/bulletins/august-2021-bulletin	O-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.com/company/product-security/bulletins/august-2021-bulletin	O-QUA-SA81-200921/3163
Incorrect Type	08-Sep-21	4.6	Incorrect pointer argument passed to trusted application	https://www.qualcomm.co	O-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/bulletins/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.com/company/product-security/bulletins/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.com/company/product-security/bulletins/august-2021-bulletin	O-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.com/company/product-security/bulletins/august-2021-bulletin	O-QUA-SA81-200921/3167

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1972**		
sa8155p_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.com/company/product-security/bulletins/august-2021-bulletin	O-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.com/company/product-security/bulletins/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.com/company/product-security/bull	O-QUA-SA81-200921/3170

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 Wraparound)	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.com/company/product-security/bulletins/august-2021-bulletin	O-QUA-SA81-200921/3171
Integer Underflow (Wrap or Wraparound)	08-Sep-21	10	Integer underflow can occur due to improper 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.com/company/product-security/bulletins/august-2021-bulletin	O-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.com/company/product-security/bulletins/august-	O-QUA-SA81-200921/3173

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.com/company/product-security/bulletins/august-2021-bulletin	O-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.com/company/product-security/bulletins/august-2021-bulletin	O-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 Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking	https://www.qualcomm.com/company/product-security/bulletins/august-2021-bulletin	O-QUA-SA81-200921/3176

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2021-1972		
sa8155_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.com/company/product-security/bulletins/august-2021-bulletin	O-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.com/company/product-security/bulletins/august-2021-bulletin	O-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.com/company/product-security/bulletins/august-2021-bulletin	O-QUA-SA81-200921/3179

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 Wraparound)	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.com/company/product-security/bulletins/august-2021-bulletin	O-QUA-SA81-200921/3180
Integer Underflow (Wrap or Wraparound)	08-Sep-21	10	Integer underflow can occur due to improper 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.com/company/product-security/bulletins/august-2021-bulletin	O-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.com/company/product-security/bulletins/august-2021-bulletin	O-QUA-SA81-200921/3182

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.com/company/product-security/bulletins/august-2021-bulletin	O-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.com/company/product-security/bulletins/august-2021-bulletin	O-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 Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1972**	https://www.qualcomm.com/company/product-security/bulletins/august-2021-bulletin	O-QUA-SA81-200921/3185
sa8195p_firmware					
Exposure of	08-Sep-21	2.1	Child process can leak	https://www.	O-QUA-SA81-

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 Voice & Music, Snapdragon Wearables **CVE ID : CVE-2021-1904**	qualcomm.com/company/product-security/bulletins/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.com/company/product-security/bulletins/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.com/company/product-security/bulletins/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.com/company/	O-QUA-SA81-200921/3189

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/bulletins/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.com/company/product-security/bulletins/august-2021-bulletin	O-QUA-SA81-200921/3190
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	08-Sep-21	10	Possible buffer overflow due to 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 Networking **CVE ID : CVE-2021-1972**	https://www.qualcomm.com/company/product-security/bulletins/august-2021-bulletin	O-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.com/company/product-	O-QUA-SC81-200921/3192

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/bulletins/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.com/company/product-security/bulletins/august-2021-bulletin	O-QUA-SC81-200921/3193
Integer Underflow (Wrap or Wraparound)	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.com/company/product-security/bulletins/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.com/company/product-	O-QUA-SC81-200921/3195

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/bulletins/august-2021-bulletin	
sd205_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.com/company/product-security/bulletins/august-2021-bulletin	O-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 IoT, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2021-1914**	https://www.qualcomm.com/company/product-security/bulletins/august-2021-bulletin	O-QUA-SD20-200921/3197
Out-of-bounds	08-Sep-21	10	Possible buffer underflow due to lack of check for	https://www.qualcomm.co	O-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/bulletins/august-2021-bulletin	
Integer Underflow (Wrap or Wraparound)	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.com/company/product-security/bulletins/august-2021-bulletin	O-QUA-SD20-200921/3199
Integer Underflow (Wrap or Wraparound)	08-Sep-21	10	Integer underflow can occur due to improper 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.com/company/product-security/bulletins/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.com/company/	O-QUA-SD20-200921/3201

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/bulletins/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.com/company/product-security/bulletins/august-2021-bulletin	O-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 Mobile, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1972**	https://www.qualcomm.com/company/product-security/bulletins/august-2021-bulletin	O-QUA-SD20-200921/3203
sd210_firmware					
Exposure of	08-Sep-21	2.1	Child process can leak	https://www.	O-QUA-SD21-

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 Voice & Music, Snapdragon Wearables **CVE ID : CVE-2021-1904**	qualcomm.com/company/product-security/bulletins/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.com/company/product-security/bulletins/august-2021-bulletin	O-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.com/company/product-security/bulletins/august-2021-bulletin	O-QUA-SD21-200921/3206

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2021-1916		
Integer Underflow (Wrap or Wraparound)	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.com/company/product-security/bulletins/august-2021-bulletin	O-QUA-SD21-200921/3207
Integer Underflow (Wrap or Wraparound)	08-Sep-21	10	Integer underflow can occur due to improper 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.com/company/product-security/bulletins/august-2021-bulletin	O-QUA-SD21-200921/3208
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.com/company/product-security/bulletins/august-2021-bulletin	O-QUA-SD21-200921/3209

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.com/company/product-security/bulletins/august-2021-bulletin	O-QUA-SD21-200921/3210
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	08-Sep-21	10	Possible buffer overflow due to 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 Networking **CVE ID : CVE-2021-1972**	https://www.qualcomm.com/company/product-security/bulletins/august-2021-bulletin	O-QUA-SD21-200921/3211
sd429_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,	https://www.qualcomm.com/company/product-security/bulletins/august-2021-bulletin	O-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 **CVE ID : CVE-2021-1914**	https://www.qualcomm.com/company/product-security/bulletins/august-2021-bulletin	O-QUA-SD42-200921/3213
Out-of-bounds Write	08-Sep-21	10	Possible buffer underflow due to lack of check for negative indices values when 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.com/company/product-security/bulletins/august-2021-bulletin	O-QUA-SD42-200921/3214
Integer Underflow (Wrap or Wraparound)	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.com/company/product-security/bulletins/august-2021-bulletin	O-QUA-SD42-200921/3215

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Wearables **CVE ID : CVE-2021-1919**		
Integer Underflow (Wrap or Wraparound)	08-Sep-21	10	Integer underflow can occur due to improper 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.com/company/product-security/bulletins/august-2021-bulletin	O-QUA-SD42-200921/3216
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	08-Sep-21	10	Possible buffer overflow due to 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 Networking **CVE ID : CVE-2021-1972**	https://www.qualcomm.com/company/product-security/bulletins/august-2021-bulletin	O-QUA-SD42-200921/3217
sd439_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,	https://www.qualcomm.com/company/product-security/bulletins/august-2021-bulletin	O-QUA-SD43-200921/3218

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 IoT, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2021-1914**	https://www.qualcomm.com/company/product-security/bulletins/august-2021-bulletin	O-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.com/company/product-security/bulletins/august-2021-bulletin	O-QUA-SD43-200921/3220
Integer Underflow (Wrap or Wraparound)	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.com/company/product-security/bulletins/august-	O-QUA-SD43-200921/3221

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 Wraparound)	08-Sep-21	10	Integer underflow can occur due to improper 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.com/company/product-security/bulletins/august-2021-bulletin	O-QUA-SD43-200921/3222
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	08-Sep-21	10	Possible buffer overflow due to 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 Networking **CVE ID : CVE-2021-1972**	https://www.qualcomm.com/company/product-security/bulletins/august-2021-bulletin	O-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.com/company/product-	O-QUA-SD45-200921/3224

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/bulletins/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.com/company/product-security/bulletins/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.com/company/product-security/bulletins/august-2021-bulletin	O-QUA-SD45-200921/3226
Integer Underflow	08-Sep-21	10	Integer underflow can occur when the RTCP length is	https://www.qualcomm.co	O-QUA-SD45-200921/3227

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
(Wrap or Wraparound)			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/bulletins/august-2021-bulletin	
Integer Underflow (Wrap or Wraparound)	08-Sep-21	10	Integer underflow can occur due to improper 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.com/company/product-security/bulletins/august-2021-bulletin	O-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 Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1972**	https://www.qualcomm.com/company/product-security/bulletins/august-2021-bulletin	O-QUA-SD45-200921/3229
sd460_firmware					

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.com/company/product-security/bulletins/august-2021-bulletin	O-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.com/company/product-security/bulletins/august-2021-bulletin	O-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.com/company/product-security/bulletins/august-2021-bulletin	O-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.com/company/product-	O-QUA-SD46-200921/3233

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 **CVE ID : CVE-2021-1930**	security/bulletins/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 Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1972**	https://www.qualcomm.com/company/product-security/bulletins/august-2021-bulletin	O-QUA-SD46-200921/3234
sd480_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.com/company/product-security/bulletins/august-2021-bulletin	O-QUA-SD48-200921/3235
Loop with Unreachable	08-Sep-21	5	Loop with unreachable exit condition may occur due to	https://www.qualcomm.co	O-QUA-SD48-200921/3236

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/bulletins/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.com/company/product-security/bulletins/august-2021-bulletin	O-QUA-SD48-200921/3237
Integer Underflow (Wrap or Wraparound)	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.com/company/product-security/bulletins/august-2021-bulletin	O-QUA-SD48-200921/3238
Integer Underflow	08-Sep-21	10	Integer underflow can occur due to improper handling of	https://www.qualcomm.co	O-QUA-SD48-200921/3239

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
(Wrap or Wraparound)			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/bulletins/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.com/company/product-security/bulletins/august-2021-bulletin	O-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.com/company/product-security/bulletins/august-2021-bulletin	O-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.com/company/product-security/bulletins/august-2021-bulletin	O-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 Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1972**	https://www.qualcomm.com/company/product-security/bulletins/august-2021-bulletin	O-QUA-SD48-200921/3243
sd632_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.com/company/product-security/bulletins/august-2021-bulletin	O-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.com/company/product-security/bulletins/august-	O-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.com/company/product-security/bulletins/august-2021-bulletin	O-QUA-SD63-200921/3246
Integer Underflow (Wrap or Wraparound)	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.com/company/product-security/bulletins/august-2021-bulletin	O-QUA-SD63-200921/3247
Integer Underflow (Wrap or Wraparound)	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.com/company/product-security/bulletins/august-	O-QUA-SD63-200921/3248

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 Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1972**	https://www.qualcomm.com/company/product-security/bulletins/august-2021-bulletin	O-QUA-SD63-200921/3249
sd660_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.com/company/product-security/bulletins/august-2021-bulletin	O-QUA-SD66-200921/3250
Buffer Copy without	08-Sep-21	10	Possible buffer overflow due to improper validation of	https://www.qualcomm.co	O-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 Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1972**	m/company/product-security/bulletins/august-2021-bulletin	
sd662_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.com/company/product-security/bulletins/august-2021-bulletin	O-QUA-SD66-200921/3252
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.com/company/product-security/bulletins/august-2021-bulletin	O-QUA-SD66-200921/3253
Exposure of	08-Sep-21	2.1	Lack of strict validation of	https://www.	O-QUA-SD66-

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.com/company/product-security/bulletins/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.com/company/product-security/bulletins/august-2021-bulletin	O-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 Mobile, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1972**	https://www.qualcomm.com/company/product-security/bulletins/august-2021-bulletin	O-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	O-QUA-SD66-200921/3257

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/bulletins/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.com/company/product-security/bulletins/august-2021-bulletin	O-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.com/company/product-security/bulletins/august-2021-bulletin	O-QUA-SD66-200921/3259

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Integer Underflow (Wrap or Wraparound)	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.com/company/product-security/bulletins/august-2021-bulletin	O-QUA-SD66-200921/3260
Integer Underflow (Wrap or Wraparound)	08-Sep-21	10	Integer underflow can occur due to improper 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.com/company/product-security/bulletins/august-2021-bulletin	O-QUA-SD66-200921/3261
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.com/company/product-security/bulletins/august-2021-bulletin	O-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.com/company/product-security/bull	O-QUA-SD66-200921/3263

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wearables **CVE ID : CVE-2021-1929**	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.com/company/product-security/bulletins/august-2021-bulletin	O-QUA-SD66-200921/3264
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	08-Sep-21	10	Possible buffer overflow due to 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 Networking **CVE ID : CVE-2021-1972**	https://www.qualcomm.com/company/product-security/bulletins/august-2021-bulletin	O-QUA-SD66-200921/3265
sd670_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,	https://www.qualcomm.com/company/product-security/bulletins/august-	O-QUA-SD67-200921/3266

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	
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.com/company/product-security/bulletins/august-2021-bulletin	O-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.com/company/product-security/bulletins/august-2021-bulletin	O-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.com/company/product-	O-QUA-SD67-200921/3269

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/bulletins/august-2021-bulletin	
Integer Underflow (Wrap or Wraparound)	08-Sep-21	10	Integer underflow can occur due to improper 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.com/company/product-security/bulletins/august-2021-bulletin	O-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.com/company/product-security/bulletins/august-2021-bulletin	O-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.com/company/product-security/bulletins/august-2021-bulletin	O-QUA-SD67-200921/3272

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 Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1972**	https://www.qualcomm.com/company/product-security/bulletins/august-2021-bulletin	O-QUA-SD67-200921/3273
sd675_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.com/company/product-security/bulletins/august-2021-bulletin	O-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.com/company/product-security/bulletins/august-2021-bulletin	O-QUA-SD67-200921/3275

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.com/company/product-security/bulletins/august-2021-bulletin	O-QUA-SD67-200921/3276
Integer Underflow (Wrap or Wraparound)	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.com/company/product-security/bulletins/august-2021-bulletin	O-QUA-SD67-200921/3277
Integer Underflow (Wrap or Wraparound)	08-Sep-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.com/company/product-security/bulletins/august-2021-bulletin	O-QUA-SD67-200921/3278

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.com/company/product-security/bulletins/august-2021-bulletin	O-QUA-SD67-200921/3279
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.com/company/product-security/bulletins/august-2021-bulletin	O-QUA-SD67-200921/3280
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.com/company/product-security/bulletins/august-2021-bulletin	O-QUA-SD67-200921/3281
Buffer Copy without Checking	08-Sep-21	10	Possible buffer overflow due to improper validation of device types during P2P	https://www.qualcomm.com/company/	O-QUA-SD67-200921/3282

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/bulletins/august-2021-bulletin	
sd678_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.com/company/product-security/bulletins/august-2021-bulletin	O-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.com/company/product-security/bulletins/august-2021-bulletin	O-QUA-SD67-200921/3284

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 **CVE ID : CVE-2021-1916**	https://www.qualcomm.com/company/product-security/bulletins/august-2021-bulletin	O-QUA-SD67-200921/3285
Integer Underflow (Wrap or Wraparound)	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.com/company/product-security/bulletins/august-2021-bulletin	O-QUA-SD67-200921/3286
Integer Underflow (Wrap or Wraparound)	08-Sep-21	10	Integer underflow can occur due to improper 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.com/company/product-security/bulletins/august-2021-bulletin	O-QUA-SD67-200921/3287

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.com/company/product-security/bulletins/august-2021-bulletin	O-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.com/company/product-security/bulletins/august-2021-bulletin	O-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.com/company/product-security/bulletins/august-2021-bulletin	O-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.com/company/product-security/bulletins/august-2021-bulletin	O-QUA-SD67-200921/3291

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_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.com/company/product-security/bulletins/august-2021-bulletin	O-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.com/company/product-security/bulletins/august-2021-bulletin	O-QUA-SD69-200921/3293
Out-of-bounds	08-Sep-21	10	Possible buffer underflow due to lack of check for	https://www.qualcomm.co	O-QUA-SD69-200921/3294

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/bulletins/august-2021-bulletin	
Integer Underflow (Wrap or Wraparound)	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.com/company/product-security/bulletins/august-2021-bulletin	O-QUA-SD69-200921/3295
Integer Underflow (Wrap or Wraparound)	08-Sep-21	10	Integer underflow can occur due to improper 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.com/company/product-security/bulletins/august-2021-bulletin	O-QUA-SD69-200921/3296
Incorrect Type Conversion	08-Sep-21	4.6	Incorrect pointer argument passed to trusted application TA could result in un-	https://www.qualcomm.com/company/	O-QUA-SD69-200921/3297

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/bulletins/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.com/company/product-security/bulletins/august-2021-bulletin	O-QUA-SD69-200921/3298
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	08-Sep-21	10	Possible buffer overflow due to 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 Networking **CVE ID : CVE-2021-1972**	https://www.qualcomm.com/company/product-security/bulletins/august-2021-bulletin	O-QUA-SD69-200921/3299
sd710_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,	https://www.qualcomm.com/company/product-security/bulletins/august-	O-QUA-SD71-200921/3300

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 **CVE ID : CVE-2021-1930**	https://www.qualcomm.com/company/product-security/bulletins/august-2021-bulletin	O-QUA-SD71-200921/3301
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	08-Sep-21	10	Possible buffer overflow due to 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 Networking **CVE ID : CVE-2021-1972**	https://www.qualcomm.com/company/product-security/bulletins/august-2021-bulletin	O-QUA-SD71-200921/3302
sd712_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.com/company/product-	O-QUA-SD71-200921/3303

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/bulletins/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.com/company/product-security/bulletins/august-2021-bulletin	O-QUA-SD71-200921/3304
Integer Underflow (Wrap or Wraparound)	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.com/company/product-security/bulletins/august-2021-bulletin	O-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.com/company/product-	O-QUA-SD71-200921/3306

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/bulletins/august-2021-bulletin	
sd720g_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.com/company/product-security/bulletins/august-2021-bulletin	O-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.com/company/product-security/bulletins/august-2021-bulletin	O-QUA-SD72-200921/3308
Out-of-bounds	08-Sep-21	10	Possible buffer underflow due to lack of check for	https://www.qualcomm.co	O-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/bulletins/august-2021-bulletin	
Integer Underflow (Wrap or Wraparound)	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.com/company/product-security/bulletins/august-2021-bulletin	O-QUA-SD72-200921/3310
Integer Underflow (Wrap or Wraparound)	08-Sep-21	10	Integer underflow can occur due to improper 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.com/company/product-security/bulletins/august-2021-bulletin	O-QUA-SD72-200921/3311
Incorrect Type Conversion	08-Sep-21	4.6	Incorrect pointer argument passed to trusted application TA could result in un-	https://www.qualcomm.com/company/	O-QUA-SD72-200921/3312

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/bulletins/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.com/company/product-security/bulletins/august-2021-bulletin	O-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.com/company/product-security/bulletins/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.com/company/product-security/bulletins/august-2021-bulletin	O-QUA-SD72-200921/3315

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1972**		
sd730_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.com/company/product-security/bulletins/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.com/company/product-security/bulletins/august-2021-bulletin	O-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.com/company/product-security/bulletins/august-	O-QUA-SD73-200921/3318

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-2021-1916**	2021-bulletin	
Integer Underflow (Wrap or Wraparound)	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.com/company/product-security/bulletins/august-2021-bulletin	O-QUA-SD73-200921/3319
Integer Underflow (Wrap or Wraparound)	08-Sep-21	10	Integer underflow can occur due to improper 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.com/company/product-security/bulletins/august-2021-bulletin	O-QUA-SD73-200921/3320
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.com/company/product-security/bulletins/august-2021-bulletin	O-QUA-SD73-200921/3321

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.com/company/product-security/bulletins/august-2021-bulletin	O-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.com/company/product-security/bulletins/august-2021-bulletin	O-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 Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1972**	https://www.qualcomm.com/company/product-security/bulletins/august-2021-bulletin	O-QUA-SD73-200921/3324

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
sd750g_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.com/company/product-security/bulletins/august-2021-bulletin	O-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.com/company/product-security/bulletins/august-2021-bulletin	O-QUA-SD75-200921/3326
Out-of-bounds Write	08-Sep-21	10	Possible buffer underflow due to lack of check for negative indices values 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.com/company/product-security/bulletins/august-2021-bulletin	O-QUA-SD75-200921/3327

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Wearables **CVE ID : CVE-2021-1916**		
Integer Underflow (Wrap or Wraparound)	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.com/company/product-security/bulletins/august-2021-bulletin	O-QUA-SD75-200921/3328
Integer Underflow (Wrap or Wraparound)	08-Sep-21	10	Integer underflow can occur due to improper 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.com/company/product-security/bulletins/august-2021-bulletin	O-QUA-SD75-200921/3329
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.com/company/product-security/bulletins/august-2021-bulletin	O-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.com/company/	O-QUA-SD75-200921/3331

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 **CVE ID : CVE-2021-1930**	product-security/bulletins/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 Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1972**	https://www.qualcomm.com/company/product-security/bulletins/august-2021-bulletin	O-QUA-SD75-200921/3332
sd765g_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.com/company/product-security/bulletins/august-2021-bulletin	O-QUA-SD76-200921/3333
Loop with	08-Sep-21	5	Loop with unreachable exit	https://www.	O-QUA-SD76-

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.com/company/product-security/bulletins/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 **CVE ID : CVE-2021-1916**	https://www.qualcomm.com/company/product-security/bulletins/august-2021-bulletin	O-QUA-SD76-200921/3335
Integer Underflow (Wrap or Wraparound)	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.com/company/product-security/bulletins/august-2021-bulletin	O-QUA-SD76-200921/3336
Integer	08-Sep-21	10	Integer underflow can occur	https://www.	O-QUA-SD76-

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Underflow (Wrap or Wraparound)			due to improper 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.com/company/product-security/bulletins/august-2021-bulletin	200921/3337
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.com/company/product-security/bulletins/august-2021-bulletin	O-QUA-SD76-200921/3338
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.com/company/product-security/bulletins/august-2021-bulletin	O-QUA-SD76-200921/3339
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.com/company/product-security/bulletins/august-2021-bulletin	O-QUA-SD76-200921/3340

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 Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1972**	https://www.qualcomm.com/company/product-security/bulletins/august-2021-bulletin	O-QUA-SD76-200921/3341
sd765_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.com/company/product-security/bulletins/august-2021-bulletin	O-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.com/company/product-security/bull	O-QUA-SD76-200921/3343

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.com/company/product-security/bulletins/august-2021-bulletin	O-QUA-SD76-200921/3344
Integer Underflow (Wrap or Wraparound)	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.com/company/product-security/bulletins/august-2021-bulletin	O-QUA-SD76-200921/3345
Integer Underflow (Wrap or Wraparound)	08-Sep-21	10	Integer underflow can occur due to improper handling of incoming RTCP packets in Snapdragon Auto, Snapdragon Compute,	https://www.qualcomm.com/company/product-security/bull	O-QUA-SD76-200921/3346

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-2021-1920**	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.com/company/product-security/bulletins/august-2021-bulletin	O-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.com/company/product-security/bulletins/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.com/company/product-security/bulletins/august-2021-bulletin	O-QUA-SD76-200921/3349

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 Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1972**	https://www.qualcomm.com/company/product-security/bulletins/august-2021-bulletin	O-QUA-SD76-200921/3350
sd768g_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.com/company/product-security/bulletins/august-2021-bulletin	O-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.com/company/product-security/bulletins/august-2021-bulletin	O-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 **CVE ID : CVE-2021-1916**	https://www.qualcomm.com/company/product-security/bulletins/august-2021-bulletin	O-QUA-SD76-200921/3353
Integer Underflow (Wrap or Wraparound)	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.com/company/product-security/bulletins/august-2021-bulletin	O-QUA-SD76-200921/3354
Integer Underflow (Wrap or Wraparound)	08-Sep-21	10	Integer underflow can occur 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.com/company/product-security/bulletins/august-2021-bulletin	O-QUA-SD76-200921/3355

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.com/company/product-security/bulletins/august-2021-bulletin	O-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.com/company/product-security/bulletins/august-2021-bulletin	O-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.com/company/product-security/bulletins/august-2021-bulletin	O-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.com/company/product-security/bull	O-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_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.com/company/product-security/bulletins/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.com/company/product-security/bulletins/august-2021-bulletin	O-QUA-SD77-200921/3361

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.com/company/product-security/bulletins/august-2021-bulletin	O-QUA-SD77-200921/3362
Integer Underflow (Wrap or Wraparound)	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.com/company/product-security/bulletins/august-2021-bulletin	O-QUA-SD77-200921/3363
Integer Underflow (Wrap or Wraparound)	08-Sep-21	10	Integer underflow can occur due to improper 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.com/company/product-security/bulletins/august-2021-bulletin	O-QUA-SD77-200921/3364
Incorrect	08-Sep-21	4.6	Incorrect pointer argument	https://www.	O-QUA-SD77-

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.com/company/product-security/bulletins/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.com/company/product-security/bulletins/august-2021-bulletin	O-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.com/company/product-security/bulletins/august-2021-bulletin	O-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.com/company/product-security/bulletins/august-2021-bulletin	O-QUA-SD77-200921/3368

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_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.com/company/product-security/bulletins/august-2021-bulletin	O-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.com/company/product-security/bulletins/august-2021-bulletin	O-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.com/company/product-	O-QUA-SD78-200921/3371

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/bulletins/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.com/company/product-security/bulletins/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.com/company/product-security/bulletins/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 Voice & Music, Snapdragon Wearables, Snapdragon Wired	https://www.qualcomm.com/company/product-security/bulletins/august-2021-bulletin	O-QUA-SD78-200921/3374

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Infrastructure and Networking **CVE ID : CVE-2021-1972**		
sd7c_firmware					
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.com/company/product-security/bulletins/august-2021-bulletin	O-QUA-SD7C-200921/3375
sd820_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.com/company/product-security/bulletins/august-2021-bulletin	O-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.com/company/product-security/bulletins/august-2021-bulletin	O-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 Wraparound)	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.com/company/product-security/bulletins/august-2021-bulletin	O-QUA-SD82-200921/3378
Integer Underflow (Wrap or Wraparound)	08-Sep-21	10	Integer underflow can occur due to improper 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.com/company/product-security/bulletins/august-2021-bulletin	O-QUA-SD82-200921/3379
sd821_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	https://www.qualcomm.com/company/product-security/bulletins/august-2021-bulletin	O-QUA-SD82-200921/3380

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.com/company/product-security/bulletins/august-2021-bulletin	O-QUA-SD82-200921/3381
Integer Underflow (Wrap or Wraparound)	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.com/company/product-security/bulletins/august-2021-bulletin	O-QUA-SD82-200921/3382
Integer Underflow (Wrap or Wraparound)	08-Sep-21	10	Integer underflow can occur due to improper 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.com/company/product-security/bulletins/august-2021-bulletin	O-QUA-SD82-200921/3383

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Wearables **CVE ID : CVE-2021-1920**		
sd835_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.com/company/product-security/bulletins/august-2021-bulletin	O-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 IoT, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2021-1914**	https://www.qualcomm.com/company/product-security/bulletins/august-2021-bulletin	O-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.com/company/product-security/bulletins/august-2021-bulletin	O-QUA-SD83-200921/3386

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 Wraparound)	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.com/company/product-security/bulletins/august-2021-bulletin	O-QUA-SD83-200921/3387
Integer Underflow (Wrap or Wraparound)	08-Sep-21	10	Integer underflow can occur due to improper 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.com/company/product-security/bulletins/august-2021-bulletin	O-QUA-SD83-200921/3388
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	08-Sep-21	10	Possible buffer overflow due 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.com/company/product-security/bulletins/august-2021-bulletin	O-QUA-SD83-200921/3389

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_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.com/company/product-security/bulletins/august-2021-bulletin	O-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.com/company/product-security/bulletins/august-2021-bulletin	O-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.com/company/product-	O-QUA-SD84-200921/3392

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/bulletins/august-2021-bulletin	
Integer Underflow (Wrap or Wraparound)	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.com/company/product-security/bulletins/august-2021-bulletin	O-QUA-SD84-200921/3393
Integer Underflow (Wrap or Wraparound)	08-Sep-21	10	Integer underflow can occur due to improper 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.com/company/product-security/bulletins/august-2021-bulletin	O-QUA-SD84-200921/3394
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.com/company/product-security/bull	O-QUA-SD84-200921/3395

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	
sd850_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.com/company/product-security/bulletins/august-2021-bulletin	O-QUA-SD85-200921/3396
Out-of-bounds Write	08-Sep-21	10	Possible buffer underflow due to lack of check for negative indices values when 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.com/company/product-security/bulletins/august-2021-bulletin	O-QUA-SD85-200921/3397
Integer	08-Sep-21	10	Integer underflow can occur	https://www.	O-QUA-SD85-

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Underflow (Wrap or Wraparound)			when 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.com/company/product-security/bulletins/august-2021-bulletin	200921/3398
Integer Underflow (Wrap or Wraparound)	08-Sep-21	10	Integer underflow can occur due to improper 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.com/company/product-security/bulletins/august-2021-bulletin	O-QUA-SD85-200921/3399
sd855_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.com/company/product-security/bulletins/august-2021-bulletin	O-QUA-SD85-200921/3400

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.com/company/product-security/bulletins/august-2021-bulletin	O-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.com/company/product-security/bulletins/august-2021-bulletin	O-QUA-SD85-200921/3402
Integer Underflow (Wrap or Wraparound)	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.com/company/product-security/bulletins/august-2021-bulletin	O-QUA-SD85-200921/3403

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Integer Underflow (Wrap or Wraparound)	08-Sep-21	10	Integer underflow can occur due to improper 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.com/company/product-security/bulletins/august-2021-bulletin	O-QUA-SD85-200921/3404
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.com/company/product-security/bulletins/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.com/company/product-security/bulletins/august-2021-bulletin	O-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.com/company/product-security/bulletins/august-	O-QUA-SD85-200921/3407

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 Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1972**	https://www.qualcomm.com/company/product-security/bulletins/august-2021-bulletin	O-QUA-SD85-200921/3408
sd865_5g_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.com/company/product-security/bulletins/august-2021-bulletin	O-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.com/company/product-	O-QUA-SD86-200921/3410

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/bulletins/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.com/company/product-security/bulletins/august-2021-bulletin	O-QUA-SD86-200921/3411
Integer Underflow (Wrap or Wraparound)	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.com/company/product-security/bulletins/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.com/company/product-	O-QUA-SD86-200921/3413

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/bulletins/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.com/company/product-security/bulletins/august-2021-bulletin	O-QUA-SD86-200921/3414
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.com/company/product-security/bulletins/august-2021-bulletin	O-QUA-SD86-200921/3415
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.com/company/product-security/bulletins/august-2021-bulletin	O-QUA-SD86-200921/3416

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 Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1972**	https://www.qualcomm.com/company/product-security/bulletins/august-2021-bulletin	O-QUA-SD86-200921/3417
sd870_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.com/company/product-security/bulletins/august-2021-bulletin	O-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.com/company/product-security/bulletins/august-2021-bulletin	O-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 **CVE ID : CVE-2021-1916**	https://www.qualcomm.com/company/product-security/bulletins/august-2021-bulletin	O-QUA-SD87-200921/3420
Integer Underflow (Wrap or Wraparound)	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.com/company/product-security/bulletins/august-2021-bulletin	O-QUA-SD87-200921/3421
Integer Underflow (Wrap or Wraparound)	08-Sep-21	10	Integer underflow can occur 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.com/company/product-security/bulletins/august-2021-bulletin	O-QUA-SD87-200921/3422

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.com/company/product-security/bulletins/august-2021-bulletin	O-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.com/company/product-security/bulletins/august-2021-bulletin	O-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.com/company/product-security/bulletins/august-2021-bulletin	O-QUA-SD87-200921/3425
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.com/company/product-security/bull	O-QUA-SD87-200921/3426

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_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.com/company/product-security/bulletins/august-2021-bulletin	O-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.com/company/product-security/bulletins/august-2021-bulletin	O-QUA-SD88-200921/3428

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.com/company/product-security/bulletins/august-2021-bulletin	O-QUA-SD88-200921/3429
Integer Underflow (Wrap or Wraparound)	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.com/company/product-security/bulletins/august-2021-bulletin	O-QUA-SD88-200921/3430
Integer Underflow (Wrap or Wraparound)	08-Sep-21	10	Integer underflow can occur due to improper 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.com/company/product-security/bulletins/august-2021-bulletin	O-QUA-SD88-200921/3431
Incorrect	08-Sep-21	4.6	Incorrect pointer argument	https://www.	O-QUA-SD88-

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.com/company/product-security/bulletins/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.com/company/product-security/bulletins/august-2021-bulletin	O-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.com/company/product-security/bulletins/august-2021-bulletin	O-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.com/company/product-security/bulletins/august-2021-bulletin	O-QUA-SD88-200921/3435

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**		
sd888_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.com/company/product-security/bulletins/august-2021-bulletin	O-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 Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1972**	https://www.qualcomm.com/company/product-security/bulletins/august-2021-bulletin	O-QUA-SD88-200921/3437
sda429w_firmware					

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.com/company/product-security/bulletins/august-2021-bulletin	O-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.com/company/product-security/bulletins/august-2021-bulletin	O-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.com/company/product-security/bulletins/august-2021-bulletin	O-QUA-SDA4-200921/3440

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.com/company/product-security/bulletins/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.com/company/product-security/bulletins/august-2021-bulletin	O-QUA-SDA4-200921/3442
sdm429w_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,	https://www.qualcomm.com/company/product-security/bulletins/august-2021-bulletin	O-QUA-SDM4-200921/3443

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.com/company/product-security/bulletins/august-2021-bulletin	O-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.com/company/product-security/bulletins/august-2021-bulletin	O-QUA-SDM4-200921/3445
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	08-Sep-21	10	Possible buffer overflow due to 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.com/company/product-security/bulletins/august-2021-bulletin	O-QUA-SDM4-200921/3446

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1972**		
sdm630_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.com/company/product-security/bulletins/august-2021-bulletin	O-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.com/company/product-security/bulletins/august-2021-bulletin	O-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.com/company/product-security/bull	O-QUA-SDM6-200921/3449

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 Wraparound)	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.com/company/product-security/bulletins/august-2021-bulletin	O-QUA-SDM6-200921/3450
Integer Underflow (Wrap or Wraparound)	08-Sep-21	10	Integer underflow can occur due to improper 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.com/company/product-security/bulletins/august-2021-bulletin	O-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.com/company/product-security/bulletins/august-	O-QUA-SDM6-200921/3452

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_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.com/company/product-security/bulletins/august-2021-bulletin	O-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.com/company/product-security/bulletins/august-2021-bulletin	O-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.com/company/product-security/bull	O-QUA-SDM8-200921/3455

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Wearables **CVE ID : CVE-2021-1929**	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 Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1972**	https://www.qualcomm.com/company/product-security/bulletins/august-2021-bulletin	O-QUA-SDM8-200921/3456
sdw2500_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.com/company/product-security/bulletins/august-2021-bulletin	O-QUA-SDW2-200921/3457
Loop with Unreachable	08-Sep-21	5	Loop with unreachable exit condition may occur due to	https://www.qualcomm.co	O-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/bulletins/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.com/company/product-security/bulletins/august-2021-bulletin	O-QUA-SDW2-200921/3459
Integer Underflow (Wrap or Wraparound)	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.com/company/product-security/bulletins/august-2021-bulletin	O-QUA-SDW2-200921/3460
Integer Underflow	08-Sep-21	10	Integer underflow can occur due to improper handling of	https://www.qualcomm.co	O-QUA-SDW2-200921/3461

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
(Wrap or Wraparound)			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/bulletins/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 Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1972**	https://www.qualcomm.com/company/product-security/bulletins/august-2021-bulletin	O-QUA-SDW2-200921/3462
sdx12_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,	https://www.qualcomm.com/company/product-security/bulletins/august-2021-bulletin	O-QUA-SDX1-200921/3463

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.com/company/product-security/bulletins/august-2021-bulletin	O-QUA-SDX1-200921/3464
Out-of-bounds Write	08-Sep-21	10	Possible buffer underflow due to lack of check for negative indices values when 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.com/company/product-security/bulletins/august-2021-bulletin	O-QUA-SDX1-200921/3465
Integer Underflow (Wrap or Wraparound)	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.com/company/product-security/bulletins/august-2021-bulletin	O-QUA-SDX1-200921/3466

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Wearables **CVE ID : CVE-2021-1919**		
Integer Underflow (Wrap or Wraparound)	08-Sep-21	10	Integer underflow can occur due to improper 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.com/company/product-security/bulletins/august-2021-bulletin	O-QUA-SDX1-200921/3467
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	08-Sep-21	10	Possible buffer overflow due to 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 Networking **CVE ID : CVE-2021-1972**	https://www.qualcomm.com/company/product-security/bulletins/august-2021-bulletin	O-QUA-SDX1-200921/3468
sdx20m_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,	https://www.qualcomm.com/company/product-security/bulletins/august-2021-bulletin	O-QUA-SDX2-200921/3469

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 Mobile, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1972**	https://www.qualcomm.com/company/product-security/bulletins/august-2021-bulletin	O-QUA-SDX2-200921/3470
sdx20_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.com/company/product-security/bulletins/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	O-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/bulletins/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.com/company/product-security/bulletins/august-2021-bulletin	O-QUA-SDX2-200921/3473
Integer Underflow (Wrap or Wraparound)	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.com/company/product-security/bulletins/august-2021-bulletin	O-QUA-SDX2-200921/3474
Integer Underflow	08-Sep-21	10	Integer underflow can occur due to improper handling of	https://www.qualcomm.co	O-QUA-SDX2-200921/3475

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
(Wrap or Wraparound)			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/bulletins/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 Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1972**	https://www.qualcomm.com/company/product-security/bulletins/august-2021-bulletin	O-QUA-SDX2-200921/3476
sdx24_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,	https://www.qualcomm.com/company/product-security/bulletins/august-2021-bulletin	O-QUA-SDX2-200921/3477

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.com/company/product-security/bulletins/august-2021-bulletin	O-QUA-SDX2-200921/3478
Out-of-bounds Write	08-Sep-21	10	Possible buffer underflow due to lack of check for negative indices values when 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.com/company/product-security/bulletins/august-2021-bulletin	O-QUA-SDX2-200921/3479
Integer Underflow (Wrap or Wraparound)	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.com/company/product-security/bulletins/august-2021-bulletin	O-QUA-SDX2-200921/3480

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Wearables **CVE ID : CVE-2021-1919**		
Integer Underflow (Wrap or Wraparound)	08-Sep-21	10	Integer underflow can occur due to improper 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.com/company/product-security/bulletins/august-2021-bulletin	O-QUA-SDX2-200921/3481
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.com/company/product-security/bulletins/august-2021-bulletin	O-QUA-SDX2-200921/3482
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.com/company/product-security/bulletins/august-2021-bulletin	O-QUA-SDX2-200921/3483
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.com/company/product-security/bull	O-QUA-SDX2-200921/3484

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_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.com/company/product-security/bulletins/august-2021-bulletin	O-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.com/company/product-security/bulletins/august-2021-bulletin	O-QUA-SDX5-200921/3486

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.com/company/product-security/bulletins/august-2021-bulletin	O-QUA-SDX5-200921/3487
Integer Underflow (Wrap or Wraparound)	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.com/company/product-security/bulletins/august-2021-bulletin	O-QUA-SDX5-200921/3488
Integer Underflow (Wrap or Wraparound)	08-Sep-21	10	Integer underflow can occur due to improper 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.com/company/product-security/bulletins/august-2021-bulletin	O-QUA-SDX5-200921/3489
Incorrect	08-Sep-21	4.6	Incorrect pointer argument	https://www.	O-QUA-SDX5-

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.com/company/product-security/bulletins/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.com/company/product-security/bulletins/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.com/company/product-security/bulletins/august-2021-bulletin	O-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.com/company/product-security/bulletins/august-2021-bulletin	O-QUA-SDX5-200921/3493

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_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.com/company/product-security/bulletins/august-2021-bulletin	O-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.com/company/product-security/bulletins/august-2021-bulletin	O-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.com/company/product-	O-QUA-SDX5-200921/3496

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/bulletins/august-2021-bulletin	
Integer Underflow (Wrap or Wraparound)	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.com/company/product-security/bulletins/august-2021-bulletin	O-QUA-SDX5-200921/3497
Integer Underflow (Wrap or Wraparound)	08-Sep-21	10	Integer underflow can occur due to improper 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.com/company/product-security/bulletins/august-2021-bulletin	O-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.com/company/product-security/bull	O-QUA-SDX5-200921/3499

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.com/company/product-security/bulletins/august-2021-bulletin	O-QUA-SDX5-200921/3500
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.com/company/product-security/bulletins/august-2021-bulletin	O-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 Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and	https://www.qualcomm.com/company/product-security/bulletins/august-2021-bulletin	O-QUA-SDX5-200921/3502

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 Voice & Music, Snapdragon Wearables **CVE ID : CVE-2021-1904**	https://www.qualcomm.com/company/product-security/bulletins/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 IoT, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2021-1914**	https://www.qualcomm.com/company/product-security/bulletins/august-2021-bulletin	O-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.com/company/product-security/bulletins/august-2021-bulletin	O-QUA-SDX5-200921/3505

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 Wraparound)	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.com/company/product-security/bulletins/august-2021-bulletin	O-QUA-SDX5-200921/3506
Integer Underflow (Wrap or Wraparound)	08-Sep-21	10	Integer underflow can occur due to improper 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.com/company/product-security/bulletins/august-2021-bulletin	O-QUA-SDX5-200921/3507
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.com/company/product-security/bulletins/august-2021-bulletin	O-QUA-SDX5-200921/3508

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.com/company/product-security/bulletins/august-2021-bulletin	O-QUA-SDX5-200921/3509
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.com/company/product-security/bulletins/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 Mobile, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1972**	https://www.qualcomm.com/company/product-security/bulletins/august-2021-bulletin	O-QUA-SDX5-200921/3511
sdxr1_firmware					
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 Voice & Music, Snapdragon Wearables **CVE ID : CVE-2021-1904**	qualcomm.com/company/product-security/bulletins/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.com/company/product-security/bulletins/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.com/company/product-security/bulletins/august-2021-bulletin	O-QUA-SDXR-200921/3514

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2021-1916		
Integer Underflow (Wrap or Wraparound)	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.com/company/product-security/bulletins/august-2021-bulletin	O-QUA-SDXR-200921/3515
Integer Underflow (Wrap or Wraparound)	08-Sep-21	10	Integer underflow can occur due to improper 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.com/company/product-security/bulletins/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 Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and	https://www.qualcomm.com/company/product-security/bulletins/august-2021-bulletin	O-QUA-SDXR-200921/3517

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Networking **CVE ID : CVE-2021-1972**		
sdxr2_5g_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.com/company/product-security/bulletins/august-2021-bulletin	O-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 IoT, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2021-1914**	https://www.qualcomm.com/company/product-security/bulletins/august-2021-bulletin	O-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.com/company/product-security/bulletins/august-2021-bulletin	O-QUA-SDXR-200921/3520

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 Wraparound)	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.com/company/product-security/bulletins/august-2021-bulletin	O-QUA-SDXR-200921/3521
Integer Underflow (Wrap or Wraparound)	08-Sep-21	10	Integer underflow can occur due to improper 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.com/company/product-security/bulletins/august-2021-bulletin	O-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.com/company/product-security/bulletins/august-2021-bulletin	O-QUA-SDXR-200921/3523

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.com/company/product-security/bulletins/august-2021-bulletin	O-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.com/company/product-security/bulletins/august-2021-bulletin	O-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 Mobile, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1972**	https://www.qualcomm.com/company/product-security/bulletins/august-2021-bulletin	O-QUA-SDXR-200921/3526
sd_455_firmware					
Exposure of	08-Sep-21	2.1	Child process can leak	https://www.	O-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 Voice & Music, Snapdragon Wearables **CVE ID : CVE-2021-1904**	qualcomm.com/company/product-security/bulletins/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.com/company/product-security/bulletins/august-2021-bulletin	O-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.com/company/product-security/bulletins/august-2021-bulletin	O-QUA-SD_4-200921/3529

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2021-1916		
Integer Underflow (Wrap or Wraparound)	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.com/company/product-security/bulletins/august-2021-bulletin	O-QUA-SD_4-200921/3530
Integer Underflow (Wrap or Wraparound)	08-Sep-21	10	Integer underflow can occur due to improper 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.com/company/product-security/bulletins/august-2021-bulletin	O-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 Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and	https://www.qualcomm.com/company/product-security/bulletins/august-2021-bulletin	O-QUA-SD_4-200921/3532

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Networking **CVE ID : CVE-2021-1972**		
sd_636_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.com/company/product-security/bulletins/august-2021-bulletin	O-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.com/company/product-security/bulletins/august-2021-bulletin	O-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.com/company/product-security/bulletins/august-2021-bulletin	O-QUA-SD_6-200921/3535

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 Wraparound)	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.com/company/product-security/bulletins/august-2021-bulletin	O-QUA-SD_6-200921/3536
Integer Underflow (Wrap or Wraparound)	08-Sep-21	10	Integer underflow can occur due to improper 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.com/company/product-security/bulletins/august-2021-bulletin	O-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.com/company/product-security/bulletins/august-2021-bulletin	O-QUA-SD_6-200921/3538

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_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.com/company/product-security/bulletins/august-2021-bulletin	O-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.com/company/product-security/bulletins/august-2021-bulletin	O-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.com/company/product-	O-QUA-SD_6-200921/3541

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/bulletins/august-2021-bulletin	
Integer Underflow (Wrap or Wraparound)	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.com/company/product-security/bulletins/august-2021-bulletin	O-QUA-SD_6-200921/3542
Integer Underflow (Wrap or Wraparound)	08-Sep-21	10	Integer underflow can occur due to improper 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.com/company/product-security/bulletins/august-2021-bulletin	O-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.com/company/product-security/bull	O-QUA-SD_6-200921/3544

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.com/company/product-security/bulletins/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	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.com/company/product-security/bulletins/august-2021-bulletin	O-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 Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and	https://www.qualcomm.com/company/product-security/bulletins/august-2021-bulletin	O-QUA-SD_6-200921/3547

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Networking **CVE ID : CVE-2021-1972**		
sd_8cx_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.com/company/product-security/bulletins/august-2021-bulletin	O-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.com/company/product-security/bulletins/august-2021-bulletin	O-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.com/company/product-security/bulletins/august-2021-bulletin	O-QUA-SD_8-200921/3550

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 Wraparound)	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.com/company/product-security/bulletins/august-2021-bulletin	O-QUA-SD_8-200921/3551
Integer Underflow (Wrap or Wraparound)	08-Sep-21	10	Integer underflow can occur due to improper 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.com/company/product-security/bulletins/august-2021-bulletin	O-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.com/company/product-security/bulletins/august-2021-bulletin	O-QUA-SD_8-200921/3553

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 Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1972**	https://www.qualcomm.com/company/product-security/bulletins/august-2021-bulletin	O-QUA-SD_8-200921/3554
sd_8c_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.com/company/product-security/bulletins/august-2021-bulletin	O-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.com/company/product-security/bulletins/august-2021-bulletin	O-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.com/company/product-security/bulletins/august-2021-bulletin	O-QUA-SD_8-200921/3557
Integer Underflow (Wrap or Wraparound)	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.com/company/product-security/bulletins/august-2021-bulletin	O-QUA-SD_8-200921/3558
Integer Underflow (Wrap or Wraparound)	08-Sep-21	10	Integer underflow can occur 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.com/company/product-security/bulletins/august-2021-bulletin	O-QUA-SD_8-200921/3559

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.com/company/product-security/bulletins/august-2021-bulletin	O-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 Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1972**	https://www.qualcomm.com/company/product-security/bulletins/august-2021-bulletin	O-QUA-SD_8-200921/3561
sm4125_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,	https://www.qualcomm.com/company/product-security/bulletins/august-2021-bulletin	O-QUA-SM41-200921/3562

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables **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.com/company/product-security/bulletins/august-2021-bulletin	O-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 **CVE ID : CVE-2021-1930**	https://www.qualcomm.com/company/product-security/bulletins/august-2021-bulletin	O-QUA-SM41-200921/3564
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	08-Sep-21	10	Possible buffer overflow due to 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 Networking **CVE ID : CVE-2021-1972**	https://www.qualcomm.com/company/product-security/bulletins/august-2021-bulletin	O-QUA-SM41-200921/3565

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
sm6250p_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.com/company/product-security/bulletins/august-2021-bulletin	O-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.com/company/product-security/bulletins/august-2021-bulletin	O-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.com/company/product-security/bulletins/august-2021-bulletin	O-QUA-SM62-200921/3568

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Wearables **CVE ID : CVE-2021-1916**		
Integer Underflow (Wrap or Wraparound)	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.com/company/product-security/bulletins/august-2021-bulletin	O-QUA-SM62-200921/3569
Integer Underflow (Wrap or Wraparound)	08-Sep-21	10	Integer underflow can occur due to improper 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.com/company/product-security/bulletins/august-2021-bulletin	O-QUA-SM62-200921/3570
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.com/company/product-security/bulletins/august-2021-bulletin	O-QUA-SM62-200921/3571
Buffer Copy without	08-Sep-21	10	Possible buffer overflow due to improper validation of	https://www.qualcomm.co	O-QUA-SM62-

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 Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1972**	m/company/product-security/bulletins/august-2021-bulletin	200921/3572
sm6250_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.com/company/product-security/bulletins/august-2021-bulletin	O-QUA-SM62-200921/3573
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.com/company/product-security/bulletins/august-2021-bulletin	O-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, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon IoT, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2021-1916**	https://www.qualcomm.com/company/product-security/bulletins/august-2021-bulletin	O-QUA-SM62-200921/3575
Integer Underflow (Wrap or Wraparound)	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.com/company/product-security/bulletins/august-2021-bulletin	O-QUA-SM62-200921/3576
Integer Underflow (Wrap or Wraparound)	08-Sep-21	10	Integer underflow can occur due to improper 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.com/company/product-security/bulletins/august-2021-bulletin	O-QUA-SM62-200921/3577

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.com/company/product-security/bulletins/august-2021-bulletin	O-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.com/company/product-security/bulletins/august-2021-bulletin	O-QUA-SM62-200921/3579
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.com/company/product-security/bulletins/august-2021-bulletin	O-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.com/company/product-security/bulletins/august-2021-bulletin	O-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_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.com/company/product-security/bulletins/august-2021-bulletin	O-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.com/company/product-security/bulletins/august-2021-bulletin	O-QUA-SM72-200921/3583
Out-of-bounds	08-Sep-21	10	Possible buffer underflow due to lack of check for	https://www.qualcomm.co	O-QUA-SM72-200921/3584

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/bulletins/august-2021-bulletin	
Integer Underflow (Wrap or Wraparound)	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.com/company/product-security/bulletins/august-2021-bulletin	O-QUA-SM72-200921/3585
Integer Underflow (Wrap or Wraparound)	08-Sep-21	10	Integer underflow can occur due to improper 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.com/company/product-security/bulletins/august-2021-bulletin	O-QUA-SM72-200921/3586
Incorrect Type Conversion	08-Sep-21	4.6	Incorrect pointer argument passed to trusted application TA could result in un-	https://www.qualcomm.com/company/	O-QUA-SM72-200921/3587

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/bulletins/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.com/company/product-security/bulletins/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.com/company/product-security/bulletins/august-2021-bulletin	O-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.com/company/product-security/bulletins/august-2021-bulletin	O-QUA-SM72-200921/3590

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1972**		
sm7325_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.com/company/product-security/bulletins/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.com/company/product-security/bulletins/august-2021-bulletin	O-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.com/company/product-security/bulletins/august-2021-bulletin	O-QUA-SM73-200921/3593

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.com/company/product-security/bulletins/august-2021-bulletin	O-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 Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1972**	https://www.qualcomm.com/company/product-security/bulletins/august-2021-bulletin	O-QUA-SM73-200921/3595
wcd9306_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,	https://www.qualcomm.com/company/product-security/bulletins/august-2021-bulletin	O-QUA-WCD9-200921/3596

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.com/company/product-security/bulletins/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.com/company/product-security/bulletins/august-2021-bulletin	O-QUA-WCD9-200921/3598
Integer Underflow (Wrap or Wraparound)	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.com/company/product-security/bulletins/august-2021-bulletin	O-QUA-WCD9-200921/3599

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Voice & Music, Snapdragon Wearables **CVE ID : CVE-2021-1919**		
Integer Underflow (Wrap or Wraparound)	08-Sep-21	10	Integer underflow can occur due to improper 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.com/company/product-security/bulletins/august-2021-bulletin	O-QUA-WCD9-200921/3600
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	08-Sep-21	10	Possible buffer overflow due to 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 Networking **CVE ID : CVE-2021-1972**	https://www.qualcomm.com/company/product-security/bulletins/august-2021-bulletin	O-QUA-WCD9-200921/3601
wcd9326_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,	https://www.qualcomm.com/company/product-security/bulletins/august-2021-bulletin	O-QUA-WCD9-200921/3602

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 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.com/company/product-security/bulletins/august-2021-bulletin	O-QUA-WCD9-200921/3603
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.com/company/product-security/bulletins/august-2021-bulletin	O-QUA-WCD9-200921/3604
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.com/company/product-security/bulletins/august-2021-bulletin	O-QUA-WCD9-200921/3605

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 Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1972**	https://www.qualcomm.com/company/product-security/bulletins/august-2021-bulletin	O-QUA-WCD9-200921/3606
wcd9330_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.com/company/product-security/bulletins/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.com/company/product-security/bull	O-QUA-WCD9-200921/3608

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.com/company/product-security/bulletins/august-2021-bulletin	O-QUA-WCD9-200921/3609
Integer Underflow (Wrap or Wraparound)	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.com/company/product-security/bulletins/august-2021-bulletin	O-QUA-WCD9-200921/3610
Integer Underflow (Wrap or Wraparound)	08-Sep-21	10	Integer underflow can occur due to improper handling of incoming RTCP packets in Snapdragon Auto, Snapdragon Compute,	https://www.qualcomm.com/company/product-security/bull	O-QUA-WCD9-200921/3611

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-2021-1920**	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.com/company/product-security/bulletins/august-2021-bulletin	O-QUA-WCD9-200921/3612
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	08-Sep-21	10	Possible buffer overflow due to 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 Networking **CVE ID : CVE-2021-1972**	https://www.qualcomm.com/company/product-security/bulletins/august-2021-bulletin	O-QUA-WCD9-200921/3613
wcd9335_firmware					
Exposure of Resource to	08-Sep-21	2.1	Child process can leak information from parent	https://www.qualcomm.co	O-QUA-WCD9-

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/bulletins/august-2021-bulletin	200921/3614
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	08-Sep-21	10	Possible buffer overflow due to 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 Networking **CVE ID : CVE-2021-1972**	https://www.qualcomm.com/company/product-security/bulletins/august-2021-bulletin	O-QUA-WCD9-200921/3615
wcd9340_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,	https://www.qualcomm.com/company/product-security/bulletins/august-2021-bulletin	O-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.com/company/product-security/bulletins/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 **CVE ID : CVE-2021-1916**	https://www.qualcomm.com/company/product-security/bulletins/august-2021-bulletin	O-QUA-WCD9-200921/3618
Integer Underflow (Wrap or Wraparound)	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.com/company/product-security/bulletins/august-2021-bulletin	O-QUA-WCD9-200921/3619

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Voice & Music, Snapdragon Wearables **CVE ID : CVE-2021-1919**		
Integer Underflow (Wrap or Wraparound)	08-Sep-21	10	Integer underflow can occur due to improper 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.com/company/product-security/bulletins/august-2021-bulletin	O-QUA-WCD9-200921/3620
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.com/company/product-security/bulletins/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.com/company/product-security/bulletins/august-2021-bulletin	O-QUA-WCD9-200921/3622

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.com/company/product-security/bulletins/august-2021-bulletin	O-QUA-WCD9-200921/3623
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	08-Sep-21	10	Possible buffer overflow due to 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 Networking **CVE ID : CVE-2021-1972**	https://www.qualcomm.com/company/product-security/bulletins/august-2021-bulletin	O-QUA-WCD9-200921/3624
wcd9341_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,	https://www.qualcomm.com/company/product-security/bulletins/august-2021-bulletin	O-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.com/company/product-security/bulletins/august-2021-bulletin	O-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.com/company/product-security/bulletins/august-2021-bulletin	O-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 Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1972**	https://www.qualcomm.com/company/product-security/bulletins/august-2021-bulletin	O-QUA-WCD9-200921/3628

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
wcd9360_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.com/company/product-security/bulletins/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.com/company/product-security/bulletins/august-2021-bulletin	O-QUA-WCD9-200921/3630
Integer Underflow (Wrap or Wraparound)	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.com/company/product-security/bulletins/august-2021-bulletin	O-QUA-WCD9-200921/3631

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2021-1919		
Integer Underflow (Wrap or Wraparound)	08-Sep-21	10	Integer underflow can occur due to improper 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.com/company/product-security/bulletins/august-2021-bulletin	O-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.com/company/product-security/bulletins/august-2021-bulletin	O-QUA-WCD9-200921/3633
wcd9370_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.com/company/product-security/bulletins/august-2021-bulletin	O-QUA-WCD9-200921/3634

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.com/company/product-security/bulletins/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.com/company/product-security/bulletins/august-2021-bulletin	O-QUA-WCD9-200921/3636
Integer Underflow (Wrap or Wraparound)	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.com/company/product-security/bulletins/august-2021-bulletin	O-QUA-WCD9-200921/3637

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Integer Underflow (Wrap or Wraparound)	08-Sep-21	10	Integer underflow can occur due to improper 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.com/company/product-security/bulletins/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.com/company/product-security/bulletins/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.com/company/product-security/bulletins/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.com/company/product-security/bulletins/august-	O-QUA-WCD9-200921/3641

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 Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1972**	https://www.qualcomm.com/company/product-security/bulletins/august-2021-bulletin	O-QUA-WCD9-200921/3642
wcd9371_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.com/company/product-security/bulletins/august-2021-bulletin	O-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.com/company/product-	O-QUA-WCD9-200921/3644

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/bulletins/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.com/company/product-security/bulletins/august-2021-bulletin	O-QUA-WCD9-200921/3645
Integer Underflow (Wrap or Wraparound)	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.com/company/product-security/bulletins/august-2021-bulletin	O-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.com/company/product-	O-QUA-WCD9-200921/3647

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/bulletins/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.com/company/product-security/bulletins/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 Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1972**	https://www.qualcomm.com/company/product-security/bulletins/august-2021-bulletin	O-QUA-WCD9-200921/3649
wcd9375_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.com/company/product-	O-QUA-WCD9-200921/3650

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/bulletins/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.com/company/product-security/bulletins/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.com/company/product-security/bulletins/august-2021-bulletin	O-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-

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
(Wrap or Wraparound)			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/bulletins/august-2021-bulletin	200921/3653
Integer Underflow (Wrap or Wraparound)	08-Sep-21	10	Integer underflow can occur due to improper 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.com/company/product-security/bulletins/august-2021-bulletin	O-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.com/company/product-security/bulletins/august-2021-bulletin	O-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.com/company/product-security/bulletins/august-2021-bulletin	O-QUA-WCD9-200921/3656

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.com/company/product-security/bulletins/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 Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1972**	https://www.qualcomm.com/company/product-security/bulletins/august-2021-bulletin	O-QUA-WCD9-200921/3658
wcd9380_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,	https://www.qualcomm.com/company/product-security/bulletins/august-2021-bulletin	O-QUA-WCD9-200921/3659

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 IoT, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2021-1914**	https://www.qualcomm.com/company/product-security/bulletins/august-2021-bulletin	O-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.com/company/product-security/bulletins/august-2021-bulletin	O-QUA-WCD9-200921/3661
Integer Underflow (Wrap or Wraparound)	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.com/company/product-security/bulletins/august-	O-QUA-WCD9-200921/3662

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 Wraparound)	08-Sep-21	10	Integer underflow can occur due to improper 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.com/company/product-security/bulletins/august-2021-bulletin	O-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.com/company/product-security/bulletins/august-2021-bulletin	O-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.com/company/product-security/bulletins/august-2021-bulletin	O-QUA-WCD9-200921/3665

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.com/company/product-security/bulletins/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 Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1972**	https://www.qualcomm.com/company/product-security/bulletins/august-2021-bulletin	O-QUA-WCD9-200921/3667
wcd9385_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,	https://www.qualcomm.com/company/product-security/bulletins/august-2021-bulletin	O-QUA-WCD9-200921/3668

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.com/company/product-security/bulletins/august-2021-bulletin	O-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.com/company/product-security/bulletins/august-2021-bulletin	O-QUA-WCD9-200921/3670
Integer Underflow (Wrap or Wraparound)	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.com/company/product-security/bulletins/august-2021-bulletin	O-QUA-WCD9-200921/3671

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Wearables **CVE ID : CVE-2021-1919**		
Integer Underflow (Wrap or Wraparound)	08-Sep-21	10	Integer underflow can occur due to improper 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.com/company/product-security/bulletins/august-2021-bulletin	O-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.com/company/product-security/bulletins/august-2021-bulletin	O-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.com/company/product-security/bulletins/august-2021-bulletin	O-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.com/company/product-	O-QUA-WCD9-200921/3675

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 **CVE ID : CVE-2021-1930**	security/bulletins/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 Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1972**	https://www.qualcomm.com/company/product-security/bulletins/august-2021-bulletin	O-QUA-WCD9-200921/3676
wcn3610_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.com/company/product-security/bulletins/august-2021-bulletin	O-QUA-WCN3-200921/3677
Loop with Unreachable	08-Sep-21	5	Loop with unreachable exit condition may occur due to	https://www.qualcomm.co	O-QUA-WCN3-

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/bulletins/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.com/company/product-security/bulletins/august-2021-bulletin	O-QUA-WCN3-200921/3679
Integer Underflow (Wrap or Wraparound)	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.com/company/product-security/bulletins/august-2021-bulletin	O-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-

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
(Wrap or Wraparound)			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/bulletins/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.com/company/product-security/bulletins/august-2021-bulletin	O-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.com/company/product-security/bulletins/august-2021-bulletin	O-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.com/company/product-	O-QUA-WCN3-200921/3684

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/bulletins/august-2021-bulletin	
wcn3615_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.com/company/product-security/bulletins/august-2021-bulletin	O-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.com/company/product-security/bulletins/august-2021-bulletin	O-QUA-WCN3-200921/3686

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.com/company/product-security/bulletins/august-2021-bulletin	O-QUA-WCN3-200921/3687
Integer Underflow (Wrap or Wraparound)	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.com/company/product-security/bulletins/august-2021-bulletin	O-QUA-WCN3-200921/3688
Integer Underflow (Wrap or Wraparound)	08-Sep-21	10	Integer underflow can occur due to improper 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.com/company/product-security/bulletins/august-2021-bulletin	O-QUA-WCN3-200921/3689

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.com/company/product-security/bulletins/august-2021-bulletin	O-QUA-WCN3-200921/3690
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	08-Sep-21	10	Possible buffer overflow due to 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 Networking **CVE ID : CVE-2021-1972**	https://www.qualcomm.com/company/product-security/bulletins/august-2021-bulletin	O-QUA-WCN3-200921/3691
wcn3620_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,	https://www.qualcomm.com/company/product-security/bulletins/august-2021-bulletin	O-QUA-WCN3-200921/3692

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.com/company/product-security/bulletins/august-2021-bulletin	O-QUA-WCN3-200921/3693
Out-of-bounds Write	08-Sep-21	10	Possible buffer underflow due to lack of check for negative indices values when 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.com/company/product-security/bulletins/august-2021-bulletin	O-QUA-WCN3-200921/3694
Integer Underflow (Wrap or Wraparound)	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.com/company/product-security/bulletins/august-2021-bulletin	O-QUA-WCN3-200921/3695

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Wearables **CVE ID : CVE-2021-1919**		
Integer Underflow (Wrap or Wraparound)	08-Sep-21	10	Integer underflow can occur due to improper 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.com/company/product-security/bulletins/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.com/company/product-security/bulletins/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.com/company/product-security/bulletins/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 Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1972**	https://www.qualcomm.com/company/product-security/bulletins/august-2021-bulletin	O-QUA-WCN3-200921/3699
wcn3660b_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.com/company/product-security/bulletins/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.com/company/product-security/bulletins/august-2021-bulletin	O-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 **CVE ID : CVE-2021-1916**	https://www.qualcomm.com/company/product-security/bulletins/august-2021-bulletin	O-QUA-WCN3-200921/3702
Integer Underflow (Wrap or Wraparound)	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.com/company/product-security/bulletins/august-2021-bulletin	O-QUA-WCN3-200921/3703
Integer Underflow (Wrap or Wraparound)	08-Sep-21	10	Integer underflow can occur 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.com/company/product-security/bulletins/august-2021-bulletin	O-QUA-WCN3-200921/3704

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.com/company/product-security/bulletins/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.com/company/product-security/bulletins/august-2021-bulletin	O-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.com/company/product-security/bulletins/august-2021-bulletin	O-QUA-WCN3-200921/3707

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1972**		
wcn3660_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.com/company/product-security/bulletins/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 IoT, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2021-1914**	https://www.qualcomm.com/company/product-security/bulletins/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.com/company/product-security/bulletins/august-	O-QUA-WCN3-200921/3710

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-2021-1916**	2021-bulletin	
Integer Underflow (Wrap or Wraparound)	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.com/company/product-security/bulletins/august-2021-bulletin	O-QUA-WCN3-200921/3711
Integer Underflow (Wrap or Wraparound)	08-Sep-21	10	Integer underflow can occur due to improper 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.com/company/product-security/bulletins/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.com/company/product-security/bulletins/august-2021-bulletin	O-QUA-WCN3-200921/3713

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_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.com/company/product-security/bulletins/august-2021-bulletin	O-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.com/company/product-security/bulletins/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-

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/bulletins/august-2021-bulletin	200921/3716
Integer Underflow (Wrap or Wraparound)	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.com/company/product-security/bulletins/august-2021-bulletin	O-QUA-WCN3-200921/3717
Integer Underflow (Wrap or Wraparound)	08-Sep-21	10	Integer underflow can occur due to improper 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.com/company/product-security/bulletins/august-2021-bulletin	O-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.com/company/	O-QUA-WCN3-200921/3719

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/bulletins/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 Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1972**	https://www.qualcomm.com/company/product-security/bulletins/august-2021-bulletin	O-QUA-WCN3-200921/3720
wcn3680_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,	https://www.qualcomm.com/company/product-security/bulletins/august-2021-bulletin	O-QUA-WCN3-200921/3721

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.com/company/product-security/bulletins/august-2021-bulletin	O-QUA-WCN3-200921/3722
Out-of-bounds Write	08-Sep-21	10	Possible buffer underflow due to lack of check for negative indices values when 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.com/company/product-security/bulletins/august-2021-bulletin	O-QUA-WCN3-200921/3723
Integer Underflow (Wrap or Wraparound)	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.com/company/product-security/bulletins/august-2021-bulletin	O-QUA-WCN3-200921/3724

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Wearables **CVE ID : CVE-2021-1919**		
Integer Underflow (Wrap or Wraparound)	08-Sep-21	10	Integer underflow can occur due to improper 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.com/company/product-security/bulletins/august-2021-bulletin	O-QUA-WCN3-200921/3725
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.com/company/product-security/bulletins/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 Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and	https://www.qualcomm.com/company/product-security/bulletins/august-2021-bulletin	O-QUA-WCN3-200921/3727

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Networking **CVE ID : CVE-2021-1972**		
wcn3910_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.com/company/product-security/bulletins/august-2021-bulletin	O-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.com/company/product-security/bulletins/august-2021-bulletin	O-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.com/company/product-security/bulletins/august-2021-bulletin	O-QUA-WCN3-200921/3730

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 Wraparound)	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.com/company/product-security/bulletins/august-2021-bulletin	O-QUA-WCN3-200921/3731
Integer Underflow (Wrap or Wraparound)	08-Sep-21	10	Integer underflow can occur due to improper 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.com/company/product-security/bulletins/august-2021-bulletin	O-QUA-WCN3-200921/3732
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.com/company/product-security/bulletins/august-2021-bulletin	O-QUA-WCN3-200921/3733

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.com/company/product-security/bulletins/august-2021-bulletin	O-QUA-WCN3-200921/3734
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.com/company/product-security/bulletins/august-2021-bulletin	O-QUA-WCN3-200921/3735
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	08-Sep-21	10	Possible buffer overflow due to 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 Networking **CVE ID : CVE-2021-1972**	https://www.qualcomm.com/company/product-security/bulletins/august-2021-bulletin	O-QUA-WCN3-200921/3736
wcn3950_firmware					
Exposure of	08-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 Voice & Music, Snapdragon Wearables **CVE ID : CVE-2021-1904**	qualcomm.com/company/product-security/bulletins/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.com/company/product-security/bulletins/august-2021-bulletin	O-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.com/company/product-security/bulletins/august-2021-bulletin	O-QUA-WCN3-200921/3739

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2021-1916		
Integer Underflow (Wrap or Wraparound)	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.com/company/product-security/bulletins/august-2021-bulletin	O-QUA-WCN3-200921/3740
Integer Underflow (Wrap or Wraparound)	08-Sep-21	10	Integer underflow can occur due to improper 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.com/company/product-security/bulletins/august-2021-bulletin	O-QUA-WCN3-200921/3741
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.com/company/product-security/bulletins/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.com/company/product-	O-QUA-WCN3-200921/3743

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/bulletins/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.com/company/product-security/bulletins/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 Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1972**	https://www.qualcomm.com/company/product-security/bulletins/august-2021-bulletin	O-QUA-WCN3-200921/3745
wcn3980_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	https://www.qualcomm.com/company/product-security/bull	O-QUA-WCN3-200921/3746

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.com/company/product-security/bulletins/august-2021-bulletin	O-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.com/company/product-security/bulletins/august-2021-bulletin	O-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.com/company/product-security/bull	O-QUA-WCN3-200921/3749

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 **CVE ID : CVE-2021-1930**	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 Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1972**	https://www.qualcomm.com/company/product-security/bulletins/august-2021-bulletin	O-QUA-WCN3-200921/3750
wcn3988_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.com/company/product-security/bulletins/august-2021-bulletin	O-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.com/company/	O-QUA-WCN3-200921/3752

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/bulletins/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.com/company/product-security/bulletins/august-2021-bulletin	O-QUA-WCN3-200921/3753
Integer Underflow (Wrap or Wraparound)	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.com/company/product-security/bulletins/august-2021-bulletin	O-QUA-WCN3-200921/3754
Integer Underflow (Wrap or	08-Sep-21	10	Integer underflow can occur due to improper handling of incoming RTCP packets in	https://www.qualcomm.com/company/	O-QUA-WCN3-200921/3755

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Wraparound)			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/bulletins/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.com/company/product-security/bulletins/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.com/company/product-security/bulletins/august-2021-bulletin	O-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.com/company/product-security/bulletins/august-2021-bulletin	O-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 Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1972**	https://www.qualcomm.com/company/product-security/bulletins/august-2021-bulletin	O-QUA-WCN3-200921/3759
wcn3990_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.com/company/product-security/bulletins/august-2021-bulletin	O-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.com/company/product-security/bulletins/august-2021-bulletin	O-QUA-WCN3-200921/3761

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.com/company/product-security/bulletins/august-2021-bulletin	O-QUA-WCN3-200921/3762
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	08-Sep-21	10	Possible buffer overflow due to 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 Networking **CVE ID : CVE-2021-1972**	https://www.qualcomm.com/company/product-security/bulletins/august-2021-bulletin	O-QUA-WCN3-200921/3763
wcn3991_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,	https://www.qualcomm.com/company/product-security/bulletins/august-2021-bulletin	O-QUA-WCN3-200921/3764

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 IoT, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2021-1914**	https://www.qualcomm.com/company/product-security/bulletins/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.com/company/product-security/bulletins/august-2021-bulletin	O-QUA-WCN3-200921/3766
Integer Underflow (Wrap or Wraparound)	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.com/company/product-security/bulletins/august-	O-QUA-WCN3-200921/3767

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 Wraparound)	08-Sep-21	10	Integer underflow can occur due to improper 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.com/company/product-security/bulletins/august-2021-bulletin	O-QUA-WCN3-200921/3768
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.com/company/product-security/bulletins/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.com/company/product-security/bulletins/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.com/company/product-security/bulletins/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 Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1972**	https://www.qualcomm.com/company/product-security/bulletins/august-2021-bulletin	O-QUA-WCN3-200921/3772
wcn3998_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,	https://www.qualcomm.com/company/product-security/bulletins/august-2021-bulletin	O-QUA-WCN3-200921/3773

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.com/company/product-security/bulletins/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.com/company/product-security/bulletins/august-2021-bulletin	O-QUA-WCN3-200921/3775
Integer Underflow (Wrap or Wraparound)	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.com/company/product-security/bulletins/august-2021-bulletin	O-QUA-WCN3-200921/3776

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Wearables **CVE ID : CVE-2021-1919**		
Integer Underflow (Wrap or Wraparound)	08-Sep-21	10	Integer underflow can occur due to improper 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.com/company/product-security/bulletins/august-2021-bulletin	O-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.com/company/product-security/bulletins/august-2021-bulletin	O-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.com/company/product-security/bulletins/august-2021-bulletin	O-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.com/company/product-	O-QUA-WCN3-200921/3780

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 **CVE ID : CVE-2021-1930**	security/bulletins/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 Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1972**	https://www.qualcomm.com/company/product-security/bulletins/august-2021-bulletin	O-QUA-WCN3-200921/3781
wcn3999_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.com/company/product-security/bulletins/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-

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 Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1972**	m/company/product-security/bulletins/august-2021-bulletin	200921/3783
wcn6740_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.com/company/product-security/bulletins/august-2021-bulletin	O-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.com/company/product-security/bulletins/august-2021-bulletin	O-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.com/company/product-security/bulletins/august-2021-bulletin	O-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.com/company/product-security/bulletins/august-2021-bulletin	O-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.com/company/product-security/bulletins/august-2021-bulletin	O-QUA-WCN6-200921/3788
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.com/company/product-security/bulletins/august-	O-QUA-WCN6-200921/3789

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	
wcn6750_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.com/company/product-security/bulletins/august-2021-bulletin	O-QUA-WCN6-200921/3790
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.com/company/product-security/bulletins/august-2021-bulletin	O-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.com/company/product-security/bulletins/august-2021-bulletin	WCN6-200921/3792
Integer Underflow (Wrap or Wraparound)	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.com/company/product-security/bulletins/august-2021-bulletin	O-QUA-WCN6-200921/3793
Integer Underflow (Wrap or Wraparound)	08-Sep-21	10	Integer underflow can occur due to improper 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.com/company/product-security/bulletins/august-2021-bulletin	O-QUA-WCN6-200921/3794
Incorrect Type	08-Sep-21	4.6	Incorrect pointer argument passed to trusted application	https://www.qualcomm.co	O-QUA-WCN6-

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/bulletins/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.com/company/product-security/bulletins/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.com/company/product-security/bulletins/august-2021-bulletin	O-QUA-WCN6-200921/3797
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	08-Sep-21	10	Possible buffer overflow due to 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.com/company/product-security/bulletins/august-2021-bulletin	O-QUA-WCN6-200921/3798

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 Voice & Music, Snapdragon Wearables **CVE ID : CVE-2021-1904**	https://www.qualcomm.com/company/product-security/bulletins/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.com/company/product-security/bulletins/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.com/company/product-security/bull	O-QUA-WCN6-200921/3801

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 Wraparound)	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.com/company/product-security/bulletins/august-2021-bulletin	O-QUA-WCN6-200921/3802
Integer Underflow (Wrap or Wraparound)	08-Sep-21	10	Integer underflow can occur due to improper 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.com/company/product-security/bulletins/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.com/company/product-security/bulletins/august-	O-QUA-WCN6-200921/3804

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.com/company/product-security/bulletins/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.com/company/product-security/bulletins/august-2021-bulletin	O-QUA-WCN6-200921/3806
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	08-Sep-21	10	Possible buffer overflow due to 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 Networking	https://www.qualcomm.com/company/product-security/bulletins/august-2021-bulletin	O-QUA-WCN6-200921/3807

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2021-1972		
wcn6851_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.com/company/product-security/bulletins/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.com/company/product-security/bulletins/august-2021-bulletin	O-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.com/company/product-security/bulletins/august-2021-bulletin	O-QUA-WCN6-200921/3810

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 Wraparound)	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.com/company/product-security/bulletins/august-2021-bulletin	O-QUA-WCN6-200921/3811
Integer Underflow (Wrap or Wraparound)	08-Sep-21	10	Integer underflow can occur due to improper 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.com/company/product-security/bulletins/august-2021-bulletin	O-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.com/company/product-security/bulletins/august-2021-bulletin	O-QUA-WCN6-200921/3813

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.com/company/product-security/bulletins/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.com/company/product-security/bulletins/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 Mobile, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1972**	https://www.qualcomm.com/company/product-security/bulletins/august-2021-bulletin	O-QUA-WCN6-200921/3816
wcn6855_firmware					
Exposure of	08-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 Voice & Music, Snapdragon Wearables **CVE ID : CVE-2021-1904**	qualcomm.com/company/product-security/bulletins/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.com/company/product-security/bulletins/august-2021-bulletin	O-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.com/company/product-security/bulletins/august-2021-bulletin	O-QUA-WCN6-200921/3819

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2021-1916		
Integer Underflow (Wrap or Wraparound)	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.com/company/product-security/bulletins/august-2021-bulletin	O-QUA-WCN6-200921/3820
Integer Underflow (Wrap or Wraparound)	08-Sep-21	10	Integer underflow can occur due to improper 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.com/company/product-security/bulletins/august-2021-bulletin	O-QUA-WCN6-200921/3821
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.com/company/product-security/bulletins/august-2021-bulletin	O-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.com/company/product-	O-QUA-WCN6-200921/3823

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 **CVE ID : CVE-2021-1930**	security/bulletins/august-2021-bulletin	
wcn6856_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.com/company/product-security/bulletins/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.com/company/product-security/bulletins/august-2021-bulletin	O-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.com/company/product-	O-QUA-WCN6-200921/3826

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/bulletins/august-2021-bulletin	
Integer Underflow (Wrap or Wraparound)	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.com/company/product-security/bulletins/august-2021-bulletin	O-QUA-WCN6-200921/3827
Integer Underflow (Wrap or Wraparound)	08-Sep-21	10	Integer underflow can occur due to improper 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.com/company/product-security/bulletins/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.com/company/product-security/bull	O-QUA-WCN6-200921/3829

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.com/company/product-security/bulletins/august-2021-bulletin	O-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.com/company/product-security/bulletins/august-2021-bulletin	O-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 Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and	https://www.qualcomm.com/company/product-security/bulletins/august-2021-bulletin	O-QUA-WCN6-200921/3832

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Networking **CVE ID : CVE-2021-1972**		
whs9410_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.com/company/product-security/bulletins/august-2021-bulletin	O-QUA-WHS9-200921/3833
Out-of-bounds Write	08-Sep-21	10	Possible buffer underflow due to lack of check for negative indices values when 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.com/company/product-security/bulletins/august-2021-bulletin	O-QUA-WHS9-200921/3834
Integer Underflow (Wrap or Wraparound)	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.com/company/product-security/bulletins/august-2021-bulletin	O-QUA-WHS9-200921/3835

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Voice & Music, Snapdragon Wearables **CVE ID : CVE-2021-1919**		
Integer Underflow (Wrap or Wraparound)	08-Sep-21	10	Integer underflow can occur due to improper 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.com/company/product-security/bulletins/august-2021-bulletin	O-QUA-WHS9-200921/3836
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.com/company/product-security/bulletins/august-2021-bulletin	O-QUA-WHS9-200921/3837
wsa8810_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	https://www.qualcomm.com/company/product-security/bulletins/august-2021-bulletin	O-QUA-WSA8-200921/3838

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 IoT, Snapdragon Voice & Music, Snapdragon Wearables **CVE ID : CVE-2021-1914**	https://www.qualcomm.com/company/product-security/bulletins/august-2021-bulletin	O-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.com/company/product-security/bulletins/august-2021-bulletin	O-QUA-WSA8-200921/3840
Integer Underflow (Wrap or Wraparound)	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.com/company/product-security/bulletins/august-2021-bulletin	O-QUA-WSA8-200921/3841

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2021-1919		
Integer Underflow (Wrap or Wraparound)	08-Sep-21	10	Integer underflow can occur due to improper 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.com/company/product-security/bulletins/august-2021-bulletin	O-QUA-WSA8-200921/3842
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.com/company/product-security/bulletins/august-2021-bulletin	O-QUA-WSA8-200921/3843
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://www.qualcomm.com/company/product-security/bulletins/august-2021-bulletin	O-QUA-WSA8-200921/3844
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.com/company/	O-QUA-WSA8-200921/3845

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/bulletins/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.com/company/product-security/bulletins/august-2021-bulletin	O-QUA-WSA8-200921/3846
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	08-Sep-21	10	Possible buffer overflow due to 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 Networking **CVE ID : CVE-2021-1972**	https://www.qualcomm.com/company/product-security/bulletins/august-2021-bulletin	O-QUA-WSA8-200921/3847
wsa8815_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.com/company/product-	O-QUA-WSA8-200921/3848

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/bulletins/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.com/company/product-security/bulletins/august-2021-bulletin	O-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.com/company/product-security/bulletins/august-2021-bulletin	O-QUA-WSA8-200921/3850
Integer Underflow	08-Sep-21	10	Integer underflow can occur when the RTCP length is	https://www.qualcomm.co	O-QUA-WSA8-200921/3851

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
(Wrap or Wraparound)			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/bulletins/august-2021-bulletin	
Integer Underflow (Wrap or Wraparound)	08-Sep-21	10	Integer underflow can occur due to improper 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.com/company/product-security/bulletins/august-2021-bulletin	O-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.com/company/product-security/bulletins/august-2021-bulletin	O-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.com/company/product-security/bulletins/august-2021-bulletin	O-QUA-WSA8-200921/3854

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.com/company/product-security/bulletins/august-2021-bulletin	O-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.com/company/product-security/bulletins/august-2021-bulletin	O-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.com/company/product-security/bulletins/august-2021-bulletin	O-QUA-WSA8-200921/3857

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1972**		
wsa8830_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.com/company/product-security/bulletins/august-2021-bulletin	O-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.com/company/product-security/bulletins/august-2021-bulletin	O-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.com/company/product-security/bulletins/august-	O-QUA-WSA8-200921/3860

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-2021-1916**	2021-bulletin	
Integer Underflow (Wrap or Wraparound)	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.com/company/product-security/bulletins/august-2021-bulletin	O-QUA-WSA8-200921/3861
Integer Underflow (Wrap or Wraparound)	08-Sep-21	10	Integer underflow can occur due to improper 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.com/company/product-security/bulletins/august-2021-bulletin	O-QUA-WSA8-200921/3862
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.com/company/product-security/bulletins/august-2021-bulletin	O-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.com/company/product-security/bulletins/august-2021-bulletin	O-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.com/company/product-security/bulletins/august-2021-bulletin	O-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 Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1972**	https://www.qualcomm.com/company/product-security/bulletins/august-2021-bulletin	O-QUA-WSA8-200921/3866

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
wsa8835_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.com/company/product-security/bulletins/august-2021-bulletin	O-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.com/company/product-security/bulletins/august-2021-bulletin	O-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.com/company/product-security/bulletins/august-2021-bulletin	O-QUA-WSA8-200921/3869

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Wearables **CVE ID : CVE-2021-1916**		
Integer Underflow (Wrap or Wraparound)	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.com/company/product-security/bulletins/august-2021-bulletin	O-QUA-WSA8-200921/3870
Integer Underflow (Wrap or Wraparound)	08-Sep-21	10	Integer underflow can occur due to improper 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.com/company/product-security/bulletins/august-2021-bulletin	O-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.com/company/product-security/bulletins/august-2021-bulletin	O-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.com/company/	O-QUA-WSA8-200921/3873

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/bulletins/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.com/company/product-security/bulletins/august-2021-bulletin	O-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 Mobile, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking **CVE ID : CVE-2021-1972**	https://www.qualcomm.com/company/product-security/bulletins/august-2021-bulletin	O-QUA-WSA8-200921/3875
Schneider-electric					
accusine_pcsn_active_harmonic_filter_firmware					
Exposure of Sensitive Information	02-Sep-21	6.5	A CWE-200: Exposure of Sensitive Information to an Unauthorized Actor	https://download.schneider-	O-SCH-ACCU-200921/3876

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
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**	electric.com/files?p_Doc_Ref=SEVD-2021-222-05	
accusine_pcsp_pfvp_firmware					
Exposure of Sensitive Information to an Unauthorized 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://download.schneider-electric.com/files?p_Doc_Ref=SEVD-2021-222-05	O-SCH-ACCU-200921/3877
silabs					
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/wireless/bluetooth/bluegiga-classic-legacy-modules/device.wt32i-a	O-SIL-IWRA-200921/3878
ti					
cc256xcqfn-em_firmware					

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/product/CC2564C, https://www.ti.com/tool/CC256XC-BT-SP#primary-sw	O-TI-CC25-200921/3879
zh-jieli					
ac6901_firmware					
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/product/68-cn.html	O-ZH--AC69-200921/3880
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/product/68-cn.html	O-ZH--AC69-200921/3881

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. **CVE ID : CVE-2021-31613**	http://www.zh-jieli.com/product/68-cn.html	O-ZH--AC69-200921/3882
ac6902_firmware					
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/product/68-cn.html	O-ZH--AC69-200921/3883
ac6903_firmware					
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/product/68-cn.html	O-ZH--AC69-200921/3884

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_firmware					
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/product/68-cn.html	O-ZH--AC69-200921/3885
ac6905_firmware					
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/product/68-cn.html	O-ZH--AC69-200921/3886
ac6907_firmware					
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/product/68-cn.html	O-ZH--AC69-200921/3887

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_firmware					
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/product/68-cn.html	O-ZH--AC69-200921/3888
ac690n_firmware					
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/product/68-cn.html	O-ZH--AC69-200921/3889
ac6921_firmware					
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/product/68-	O-ZH--AC69-200921/3890

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/product/68-cn.html	O-ZH--AC69-200921/3891
ac6925_firmware					
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/product/68-cn.html	O-ZH--AC69-200921/3892

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. **CVE ID : CVE-2021-31613**	http://www.zh-jieli.com/product/68-cn.html	O-ZH--AC69-200921/3893
ac6926_firmware					
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/product/68-cn.html	O-ZH--AC69-200921/3894
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/product/68-cn.html	O-ZH--AC69-200921/3895

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_firmware					
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/product/68-cn.html	O-ZH--AC69-200921/3896
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/product/68-cn.html	O-ZH--AC69-200921/3897
ac692n_firmware					
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/product/68-cn.html	O-ZH--AC69-200921/3898

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_firmware					
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/product/68-cn.html	O-ZH--AC69-200921/3899
ac6998_firmware					
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/product/68-cn.html	O-ZH--AC69-200921/3900
ac6999_firmware					
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/product/68-	O-ZH--AC69-200921/3901

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			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**	cn.html	
fw-ac63_bt_sdk					
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	O-ZH--FW-A-200921/3902
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	N/A	O-ZH--FW-A-200921/3903

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**		