Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Application					
Anchorcms					
anchor					
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	23-04-2020	3.5	Anchor 0.12.7 allows admins to cause XSS via crafted post content. **CVE ID : CVE-2020-12071**	N/A	A-ANC-ANCH-010520/1
Apache					
heron					
Deserialization of Untrusted Data	16-04-2020	7.5	It was noticed that Apache Heron 0.20.2-incubating, Release 0.20.1-incubating, and Release v-0.20.0-incubating does not configure its YAML parser to prevent the instantiation of arbitrary types, resulting in a remote code execution vulnerabilities (CWE-502: Deserialization of Untrusted Data). **CVE ID : CVE-2020-1964**	N/A	A-APA-HERO-010520/2
app2pro					
airdisk_pro					
Improper Neutralization of Input During Web Page	24-04-2020	4.3	The AirDisk Pro app 5.5.3 for iOS allows XSS via the createFolder parameter of the Create Folder	N/A	A-APP-AIRD-010520/3

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Generation ('Cross-site Scripting')			function. **CVE ID : CVE-2020-12129**		
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	24-04-2020	4.3	The AirDisk Pro app 5.5.3 for iOS allows XSS via the deleteFile parameter of the Delete function. **CVE ID : CVE-2020-12130**	N/A	A-APP-AIRD-010520/4
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	24-04-2020	4.3	The AirDisk Pro app 5.5.3 for iOS allows XSS via the devicename parameter (shown next to the UI logo). **CVE ID : CVE-2020-12131**	N/A	A-APP-AIRD-010520/5
appinghouse					
memono					
Missing Encryption of Sensitive Data	16-04-2020	5	Users can lock their notes with a password in Memono version 3.8. Thus, users needs to know a password to read notes. However, these notes are stored in a database without encryption and an attacker can read the password-protected notes without having the password. Notes are stored in the ZENTITY table in the memono.sqlite database. **CVE ID : CVE-2020-11826**	N/A	A-APP-MEMO-010520/6
Artifex					

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
jbig2dec					
Out-of-bounds Write	27-04-2020	7.5	jbig2_image_compose in jbig2_image.c in Artifex jbig2dec before 0.18 has a heap-based buffer overflow. **CVE ID : CVE-2020-12268**	N/A	A-ART-JBIG-010520/7
Arubanetworks					
clearpass					
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	16-04-2020	3.5	ClearPass is vulnerable to Stored Cross Site Scripting by allowing a malicious administrator, or a compromised administrator account, to save malicious scripts within ClearPass that could be executed resulting in a privilege escalation attack. Resolution: Fixed in 6.7.13, 6.8.4, 6.9.0 and higher. **CVE ID : CVE-2020-7110**	N/A	A-ARU-CLEA-010520/8
Improper Neutralization of Special Elements in Output Used by a Downstream Component ('Injection')	16-04-2020	6.5	A server side injection vulnerability exists which could allow an authenticated administrative user to achieve Remote Code Execution in ClearPass. Resolution: Fixed in 6.7.13, 6.8.4, 6.9.0 and higher. **CVE ID : CVE-2020-7111**	N/A	A-ARU-CLEA-010520/9
Information Exposure	16-04-2020	4	A vulnerability was found when an attacker, while	N/A	A-ARU-CLEA-

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			communicating with the ClearPass management interface, is able to intercept and change parameters in the HTTP packets resulting in the compromise of some of ClearPass' service accounts. Resolution: Fixed in 6.7.10, 6.8.1, 6.9.0 and higher. **CVE ID : CVE-2020-7113**		010520/10
Missing Authentication for Critical Function	16-04-2020	7.5	A vulnerability exists allowing attackers, when present in the same network segment as ClearPass' management interface, to make changes to certain databases in ClearPass by crafting HTTP packets. As a result of this attack, a possible complete cluster compromise might occur. Resolution: Fixed in 6.7.13, 6.8.4, 6.9.0 and higher. **CVE ID : CVE-2020-7114**	N/A	A-ARU-CLEA-010520/11
Autodesk					
dynamo_bim					
Untrusted Search Path	17-04-2020	4.4	An improper signature validation vulnerability in Autodesk Dynamo BIM versions 2.5.1 and 2.5.0 may lead to code execution through maliciously crafted DLL files. **CVE ID : CVE-2020-7079**	N/A	A-AUT-DYNA-010520/12

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
fbx_software_development_kit					
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	17-04-2020	9.3	A buffer overflow vulnerability in the Autodesk FBX-SDK versions 2019.0 and earlier may lead to arbitrary code execution on a system running it. **CVE ID : CVE-2020-7080**	N/A	A-AUT-FBX_-010520/13
Incorrect Type Conversion or Cast	17-04-2020	9.3	A type confusion vulnerability in the Autodesk FBX-SDK versions 2019.0 and earlier may lead to arbitary code read/write on the system running it. **CVE ID : CVE-2020-7081**	N/A	A-AUT-FBX_-010520/14
Use After Free	17-04-2020	9.3	A use-after-free vulnerability in the Autodesk FBX-SDK versions 2019.0 and earlier may lead to code execution on a system running it. **CVE ID : CVE-2020-7082**	N/A	A-AUT-FBX_-010520/15
Integer Overflow or Wraparound	17-04-2020	4.3	An intager overflow vulnerability in the Autodesk FBX-SDK versions 2019.0 and earlier may lead to denial of service of the application. **CVE ID : CVE-2020-7083**	N/A	A-AUT-FBX_-010520/16
NULL Pointer Dereference	17-04-2020	4.3	A NULL pointer dereference vulnerability in the Autodesk FBX-SDK versions 2019.0 and earlier may lead to denial	N/A	A-AUT-FBX_-010520/17

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			of service of the application. **CVE ID : CVE-2020-7084**		
Out-of-bounds Write	17-04-2020	9.3	A heap overflow vulnerability in the Autodesk FBX-SDK versions 2019.2 and earlier may lead to arbitrary code execution on a system running it. **CVE ID : CVE-2020-7085**	N/A	A-AUT-FBX_-010520/18
aviatrix					
openvpn					
Improper Input Validation	16-04-2020	7.5	The Aviatrix OpenVPN client through 2.5.7 on Linux, macOS, and Windows is vulnerable when OpenSSL parameters are altered from the issued value set; the parameters could allow unauthorized third-party libraries to load. **CVE ID : CVE-2020-7224**	N/A	A-AVI-OPEN-010520/19
beakerbrowser					
beaker					
Improper Input Validation	23-04-2020	7.5	Beaker before 0.8.9 allows a sandbox escape, enabling system access and code execution. This occurs because Electron context isolation is not used, and therefore an attacker can conduct a prototype-pollution attack against the Electron internal messaging API.	N/A	A-BEA-BEAK-010520/20

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2020-12079		
bigbluebutton					
bigbluebutton					
Information Exposure	23-04-2020	5	BigBlueButton before 2.2.5 allows remote attackers to obtain sensitive files via Local File Inclusion. **CVE ID : CVE-2020-12112**	N/A	A-BIG-BIGB-010520/21
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	23-04-2020	4.3	BigBlueButton before 2.2.4 allows XSS via closed captions because dangerouslySetInnerHTML in React is used. **CVE ID : CVE-2020-12113**	N/A	A-BIG-BIGB-010520/22
bitcoin-abe_project					
bitcoin-abe					
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	20-04-2020	4.3	Abe (aka bitcoin-abe) through 0.7.2, and 0.8pre, allows XSS in __call__ in abe.py because the PATH_INFO environment variable is mishandled during a PageNotFound exception. **CVE ID : CVE-2020-11944**	N/A	A-BIT-BITC-010520/23
Bitdefender					
antivirus_2020					
Improper Link Resolution Before File Access ('Link Following')	21-04-2020	4.6	A vulnerability in the improper handling of junctions in Bitdefender Antivirus Free can allow an unprivileged user to	N/A	A-BIT-ANTI-010520/24

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			substitute a quarantined file, and restore it to a privileged location. This issue affects: Bitdefender Antivirus Free versions prior to 1.0.17. **CVE ID : CVE-2020-8099**		
bluetrace					
opentrace					
Improperly Controlled Modification of Dynamically-Determined Object Attributes	17-04-2020	5	The Cloud Functions subsystem in OpenTrace 1.0 might allow fabrication attacks by making billions of TempID requests before an AES-256-GCM key rotation occurs. **CVE ID : CVE-2020-11872**	N/A	A-BLU-OPEN-010520/25
Canonical					
ubuntu_linux					
Out-of-bounds Write	21-04-2020	6.8	re2c 1.3 has a heap-based buffer overflow in Scanner::fill in parse/scanner.cc via a long lexeme. **CVE ID : CVE-2020-11958**	N/A	A-CAN-UBUN-010520/26
cyberchimps					
gutenberg_\&_elementor_templates_importer_for_responsive					
N/A	23-04-2020	6.5	The responsive-add-ons plugin before 2.2.7 for WordPress has incorrect access control for wp-admin/admin-ajax.php?action= requests.	N/A	A-CYB-GUTE-010520/27

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2020-12073		
Dolibarr					
dolibarr					
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	16-04-2020	3.5	In Dolibarr 10.0.6, if USER_LOGIN_FAILED is active, there is a stored XSS vulnerability on the admin tools --> audit page. This may lead to stealing of the admin account. **CVE ID : CVE-2020-11823**	N/A	A-DOL-DOLI-010520/28
Cross-Site Request Forgery (CSRF)	16-04-2020	6.8	In Dolibarr 10.0.6, forms are protected with a CSRF token against CSRF attacks. The problem is any CSRF token in any user's session can be used in another user's session. CSRF tokens should not be valid in this situation. **CVE ID : CVE-2020-11825**	N/A	A-DOL-DOLI-010520/29
elementor					
elementor					
Unrestricted Upload of File with Dangerous Type	22-04-2020	9	An issue was discovered in Elementor 2.7.4. Arbitrary file upload is possible in the Elementor Import Templates function, allowing an attacker to execute code via a crafted ZIP archive. **CVE ID : CVE-2020-7055**	N/A	A-ELE-ELEM-010520/30
F5					

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
nginx_controller					
Information Exposure	23-04-2020	5.8	In versions prior to 3.3.0, the NGINX Controller is configured to communicate with its Postgres database server over unencrypted channels, making the communicated data vulnerable to interception via man-in-the-middle (MiTM) attacks. **CVE ID : CVE-2020-5865**	https://support.f5.com/csp/article/K21009022	A-F5-NGIN-010520/31
Information Exposure	23-04-2020	2.1	In versions of NGINX Controller prior to 3.3.0, the helper.sh script, which is used optionally in NGINX Controller to change settings, uses sensitive items as command-line arguments. **CVE ID : CVE-2020-5866**	https://support.f5.com/csp/article/K11922628	A-F5-NGIN-010520/32
Improper Input Validation	23-04-2020	6.8	In versions prior to 3.3.0, the NGINX Controller Agent installer script 'install.sh' uses HTTP instead of HTTPS to check and install packages **CVE ID : CVE-2020-5867**	https://support.f5.com/csp/article/K00958787	A-F5-NGIN-010520/33
big-iq_centralized_management					
Information Exposure	24-04-2020	6.4	In BIG-IQ 5.2.0-7.0.0, high availability (HA) synchronization is not secure by TLS and may allow on-path attackers to read / modify confidential data in transit. **CVE ID : CVE-2020-5869**	N/A	A-F5-BIG--010520/34

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Missing Authentication for Critical Function	24-04-2020	4.8	In BIG-IQ 5.2.0-7.0.0, high availability (HA) synchronization mechanisms do not use any form of authentication for connecting to the peer. **CVE ID : CVE-2020-5870**	N/A	A-F5-BIG--010520/35
Foxitsoftware					
phantompdf					
Access of Resource Using Incompatible Type ('Type Confusion')	22-04-2020	6.8	This vulnerability allows remote attackers to execute arbitrary code on affected installations of Foxit PhantomPDF 9.7.0.29478. User interaction is required to exploit this vulnerability in that the target must visit a malicious page or open a malicious file. The specific flaw exists within the handling of the DuplicatePages command of the communication API. The issue results from the lack of proper validation of user-supplied data, which can result in a type confusion condition. An attacker can leverage this vulnerability to execute code in the context of the current process. Was ZDI-CAN-9828. **CVE ID : CVE-2020-10889**	N/A	A-FOX-PHAN-010520/36
Cross-Site Request	22-04-2020	6.8	This vulnerability allows remote attackers to	N/A	A-FOX-PHAN-

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Forgery (CSRF)			execute arbitrary code on affected installations of Foxit PhantomPDF 9.7.0.29478. User interaction is required to exploit this vulnerability in that the target must visit a malicious page or open a malicious file. The specific flaw exists within the communication API. The issue lies in the handling of the ConvertToPDF command, which allows an arbitrary file write with attacker controlled data. An attacker can leverage this vulnerability to execute code in the context of the current process. Was ZDI-CAN-9829. **CVE ID : CVE-2020-10890**		010520/37
Access of Resource Using Incompatible Type ('Type Confusion')	22-04-2020	6.8	This vulnerability allows remote attackers to execute arbitrary code on affected installations of Foxit PhantomPDF 9.7.0.29478. User interaction is required to exploit this vulnerability in that the target must visit a malicious page or open a malicious file. The specific flaw exists within the handling of the Save command of the communication API. The issue results from the lack of proper validation of	N/A	A-FOX-PHAN-010520/38

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			user-supplied data, which can result in a type confusion condition. An attacker can leverage this vulnerability to execute code in the context of the current process. Was ZDI-CAN-9831. **CVE ID : CVE-2020-10891**		
Cross-Site Request Forgery (CSRF)	22-04-2020	6.8	This vulnerability allows remote attackers to execute arbitrary code on affected installations of Foxit PhantomPDF 9.7.0.29478. User interaction is required to exploit this vulnerability in that the target must visit a malicious page or open a malicious file. The specific flaw exists within the communication API. The issue lies in the handling of the CombineFiles command, which allows an arbitrary file write with attacker controlled data. An attacker can leverage this vulnerability to execute code in the context of the current process. Was ZDI-CAN-9830. **CVE ID : CVE-2020-10892**	N/A	A-FOX-PHAN-010520/39
Out-of-bounds Read	22-04-2020	6.8	This vulnerability allows remote attackers to execute arbitrary code on affected installations of	N/A	A-FOX-PHAN-010520/40

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Foxit PhantomPDF 9.7.1.29511. User interaction is required to exploit this vulnerability in that the target must visit a malicious page or open a malicious file. The specific flaw exists within the handling of U3D objects in PDF files. The issue results from the lack of proper validation of user-supplied data, which can result in a read past the end of an allocated structure. An attacker can leverage this vulnerability to execute code in the context of the current process. Was ZDI-CAN-10191. **CVE ID : CVE-2020-10895**		
Out-of-bounds Read	22-04-2020	6.8	This vulnerability allows remote attackers to execute arbitrary code on affected installations of Foxit PhantomPDF 9.7.1.29511. User interaction is required to exploit this vulnerability in that the target must visit a malicious page or open a malicious file. The specific flaw exists within the handling of U3D objects in PDF files. The issue results from the lack of proper validation of user-supplied data, which can result in a read past	N/A	A-FOX-PHAN-010520/41

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			the end of an allocated structure. An attacker can leverage this vulnerability to execute code in the context of the current process. Was ZDI-CAN-10195. **CVE ID : CVE-2020-10898**		
Use After Free	22-04-2020	6.8	This vulnerability allows remote attackers to execute arbitrary code on affected installations of Foxit Reader 9.7.1.29511. User interaction is required to exploit this vulnerability in that the target must visit a malicious page or open a malicious file. The specific flaw exists within the processing of XFA templates. The issue results from the lack of validating the existence of an object prior to performing operations on the object. An attacker can leverage this vulnerability to execute code in the context of the current process. Was ZDI-CAN-10132. **CVE ID : CVE-2020-10899**	N/A	A-FOX-PHAN-010520/42
Use After Free	22-04-2020	6.8	This vulnerability allows remote attackers to execute arbitrary code on affected installations of Foxit Reader 9.7.1.29511.	N/A	A-FOX-PHAN-010520/43

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			User interaction is required to exploit this vulnerability in that the target must visit a malicious page or open a malicious file. The specific flaw exists within the processing of AcroForms. The issue results from the lack of validating the existence of an object prior to performing operations on the object. An attacker can leverage this vulnerability to execute code in the context of the current process. Was ZDI-CAN-10142. **CVE ID : CVE-2020-10900**		
Out-of-bounds Read	22-04-2020	4.3	This vulnerability allows remote attackers to disclose sensitive information on affected installations of Foxit PhantomPDF 9.7.1.29511. User interaction is required to exploit this vulnerability in that the target must visit a malicious page or open a malicious file. The specific flaw exists within the handling of U3D objects embedded in a PDF. The issue results from the lack of proper validation of user-supplied data, which can result in a read past the end of an allocated	N/A	A-FOX-PHAN-010520/44

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			object. An attacker can leverage this in conjunction with other vulnerabilities to execute code in the context of the current process. Was ZDI-CAN-10463. **CVE ID : CVE-2020-10903**		
reader					
Access of Resource Using Incompatible Type ('Type Confusion')	22-04-2020	6.8	This vulnerability allows remote attackers to execute arbitrary code on affected installations of Foxit PhantomPDF 9.7.0.29478. User interaction is required to exploit this vulnerability in that the target must visit a malicious page or open a malicious file. The specific flaw exists within the handling of the DuplicatePages command of the communication API. The issue results from the lack of proper validation of user-supplied data, which can result in a type confusion condition. An attacker can leverage this vulnerability to execute code in the context of the current process. Was ZDI-CAN-9828. **CVE ID : CVE-2020-10889**	N/A	A-FOX-READ-010520/45
Cross-Site Request	22-04-2020	6.8	This vulnerability allows remote attackers to execute arbitrary code on	N/A	A-FOX-READ-

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Forgery (CSRF)			affected installations of Foxit PhantomPDF 9.7.0.29478. User interaction is required to exploit this vulnerability in that the target must visit a malicious page or open a malicious file. The specific flaw exists within the communication API. The issue lies in the handling of the ConvertToPDF command, which allows an arbitrary file write with attacker controlled data. An attacker can leverage this vulnerability to execute code in the context of the current process. Was ZDI-CAN-9829. **CVE ID : CVE-2020-10890**		010520/46
Access of Resource Using Incompatible Type ('Type Confusion')	22-04-2020	6.8	This vulnerability allows remote attackers to execute arbitrary code on affected installations of Foxit PhantomPDF 9.7.0.29478. User interaction is required to exploit this vulnerability in that the target must visit a malicious page or open a malicious file. The specific flaw exists within the handling of the Save command of the communication API. The issue results from the lack of proper validation of user-supplied data, which	N/A	A-FOX-READ-010520/47

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			can result in a type confusion condition. An attacker can leverage this vulnerability to execute code in the context of the current process. Was ZDI-CAN-9831. **CVE ID : CVE-2020-10891**		
Cross-Site Request Forgery (CSRF)	22-04-2020	6.8	This vulnerability allows remote attackers to execute arbitrary code on affected installations of Foxit PhantomPDF 9.7.0.29478. User interaction is required to exploit this vulnerability in that the target must visit a malicious page or open a malicious file. The specific flaw exists within the communication API. The issue lies in the handling of the CombineFiles command, which allows an arbitrary file write with attacker controlled data. An attacker can leverage this vulnerability to execute code in the context of the current process. Was ZDI-CAN-9830. **CVE ID : CVE-2020-10892**	N/A	A-FOX-READ-010520/48
Out-of-bounds Read	22-04-2020	6.8	This vulnerability allows remote attackers to execute arbitrary code on affected installations of Foxit PhantomPDF	N/A	A-FOX-READ-010520/49

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			9.7.1.29511. User interaction is required to exploit this vulnerability in that the target must visit a malicious page or open a malicious file. The specific flaw exists within the handling of U3D objects in PDF files. The issue results from the lack of proper validation of user-supplied data, which can result in a read past the end of an allocated structure. An attacker can leverage this vulnerability to execute code in the context of the current process. Was ZDI-CAN-10191. **CVE ID : CVE-2020-10895**		
Out-of-bounds Read	22-04-2020	6.8	This vulnerability allows remote attackers to execute arbitrary code on affected installations of Foxit PhantomPDF 9.7.1.29511. User interaction is required to exploit this vulnerability in that the target must visit a malicious page or open a malicious file. The specific flaw exists within the handling of U3D objects in PDF files. The issue results from the lack of proper validation of user-supplied data, which can result in a read past the end of an allocated	N/A	A-FOX-READ-010520/50

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			structure. An attacker can leverage this vulnerability to execute code in the context of the current process. Was ZDI-CAN-10195. **CVE ID : CVE-2020-10898**		
Use After Free	22-04-2020	6.8	This vulnerability allows remote attackers to execute arbitrary code on affected installations of Foxit Reader 9.7.1.29511. User interaction is required to exploit this vulnerability in that the target must visit a malicious page or open a malicious file. The specific flaw exists within the processing of XFA templates. The issue results from the lack of validating the existence of an object prior to performing operations on the object. An attacker can leverage this vulnerability to execute code in the context of the current process. Was ZDI-CAN-10132. **CVE ID : CVE-2020-10899**	N/A	A-FOX-READ-010520/51
Use After Free	22-04-2020	6.8	This vulnerability allows remote attackers to execute arbitrary code on affected installations of Foxit Reader 9.7.1.29511. User interaction is	N/A	A-FOX-READ-010520/52

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			required to exploit this vulnerability in that the target must visit a malicious page or open a malicious file. The specific flaw exists within the processing of AcroForms. The issue results from the lack of validating the existence of an object prior to performing operations on the object. An attacker can leverage this vulnerability to execute code in the context of the current process. Was ZDI-CAN-10142. **CVE ID : CVE-2020-10900**		
Out-of-bounds Read	22-04-2020	4.3	This vulnerability allows remote attackers to disclose sensitive information on affected installations of Foxit PhantomPDF 9.7.1.29511. User interaction is required to exploit this vulnerability in that the target must visit a malicious page or open a malicious file. The specific flaw exists within the handling of U3D objects embedded in a PDF. The issue results from the lack of proper validation of user-supplied data, which can result in a read past the end of an allocated object. An attacker can	N/A	A-FOX-READ-010520/53

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			leverage this in conjunction with other vulnerabilities to execute code in the context of the current process. Was ZDI-CAN-10463. **CVE ID : CVE-2020-10903**		
ftpdmin_project					
ftpdmin					
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	17-04-2020	5	A buffer overflow vulnerability in FTPDMIN 0.96 allows attackers to crash the server via a crafted packet. **CVE ID : CVE-2020-10813**	N/A	A-FTP-FTPD-010520/54
Gitlab					
gitlab					
Information Exposure	22-04-2020	5	An issue was discovered in GitLab Community Edition (CE) and Enterprise Edition (EE) before 12.7.9, 12.8.x before 12.8.9, and 12.9.x before 12.9.3. A Workhorse bypass could lead to NuGet package and file disclosure (Exposure of Sensitive Information) via request smuggling. **CVE ID : CVE-2020-11505**	https://about.gitlab.com/releases/2020/04/14/critical-security-release-gitlab-12-dot-9-dot-3-released/	A-GIT-GITL-010520/55
Information Exposure	22-04-2020	5	An issue was discovered in GitLab 10.7.0 and later through 12.9.2. A Workhorse bypass could	https://about.gitlab.com/releases/2020/04/14/crit	A-GIT-GITL-010520/56

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			lead to job artifact uploads and file disclosure (Exposure of Sensitive Information) via request smuggling. **CVE ID : CVE-2020-11506**	ical-security-release-gitlab-12-dot-9-dot-3-released/	
Missing Authentication for Critical Function	22-04-2020	4	An issue was discovered in GitLab CE and EE 8.15 through 12.9.2. Members of a group could still have access after the group is deleted. **CVE ID : CVE-2020-11649**	https://about.gitlab.com/releases/2020/04/14/critical-security-release-gitlab-12-dot-9-dot-3-released/	A-GIT-GITL-010520/57
Gnome					
evolution					
N/A	17-04-2020	6.4	An issue was discovered in GNOME Evolution before 3.35.91. By using the proprietary (non-RFC6068) "mailto?attach=..." parameter, a website (or other source of mailto links) can make Evolution attach local files or directories to a composed email message without showing a warning to the user, as demonstrated by an attach=. value. **CVE ID : CVE-2020-11879**	N/A	A-GNO-EVOL-010520/58
GNU					
mailman					
Improper	24-04-2020	4.3	GNU Mailman 2.x before	N/A	A-GNU-

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Neutralization of Input During Web Page Generation ('Cross-site Scripting')			2.1.30 uses the .obj extension for scrubbed application/octet-stream MIME parts. This behavior may contribute to XSS attacks against list-archive visitors, because an HTTP reply from an archive web server may lack a MIME type, and a web browser may perform MIME sniffing, conclude that the MIME type should have been text/html, and execute JavaScript code. **CVE ID : CVE-2020-12137**		MAIL-010520/59
Google					
earth					
Uncontrolled Search Path Element	21-04-2020	4.4	A vulnerability in the windows installer of Google Earth Pro versions prior to 7.3.3 allows an attacker using DLL hijacking to insert malicious local files to execute unauthenticated remote code on the targeted system. **CVE ID : CVE-2020-8895**	N/A	A-GOO-EART-010520/60
grafana					
grafana					
Improper Neutralization of Input During Web Page Generation ('Cross-site	27-04-2020	4.3	Grafana version < 6.7.3 is vulnerable for annotation popup XSS. **CVE ID : CVE-2020-12052**	https://community.grafana.com/t/release-notes-v6-7-	A-GRA-GRAF-010520/61

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Scripting')				x/27119	
gtranslate					
translate_wordpress_with_gtranslate					
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	20-04-2020	4.3	The GTranslate plugin before 2.8.52 for WordPress has Reflected XSS via a crafted link. This requires use of the hreflang tags feature within a sub-domain or sub-directory paid option. **CVE ID : CVE-2020-11930**	N/A	A-GTR-TRAN-010520/62
hcltech					
connections					
Information Exposure	22-04-2020	4	"HCL Connections is vulnerable to possible information leakage and could disclose sensitive information via stack trace to a local user." **CVE ID : CVE-2020-4085**	https://support.hcltechsw.com/csm?id=kb_article&sysparm_article=KB0077976	A-HCL-CONN-010520/63
IBM					
urbancode_deploy					
Improper Privilege Management	23-04-2020	6	IBM UrbanCode Deploy (UCD) 7.0.3.0 and 7.0.4.0 could allow an authenticated user to impersonate another user if the server is configured to enable Distributed Front End (DFE). IBM X-Force ID: 174955. **CVE ID : CVE-2020-4202**	https://www.ibm.com/support/pages/node/6195701	A-IBM-URBA-010520/64
Information Exposure	16-04-2020	4	IBM UrbanCode Deploy (UCD) 7.0.5 could allow a user with special	https://www.ibm.com/support/page	A-IBM-URBA-010520/65

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			permissions to obtain sensitive information via generic processes. IBM X-Force ID: 175639. **CVE ID : CVE-2020-4260**	s/node/6191655	
tivoli_monitoring					
Incorrect Permission Assignment for Critical Resource	23-04-2020	6.9	IBM Tivoli Monitoring 6.3.0 could allow a local attacker to execute arbitrary code on the system. By placing a specially crafted file, an attacker could exploit this vulnerability to load other DLL files located in the same directory and execute arbitrary code on the system. IBM X-Force ID: 177083. **CVE ID : CVE-2020-4311**	https://www.ibm.com/support/pages/node/6198358	A-IBM-TIVO-010520/66
maas360					
Improper Input Validation	23-04-2020	2.1	IBM MaaS360 6.82 could allow a user with pysical access to the device to crash the application which may enable the user to access restricted applications and device settings. IBM X-Force ID: 178505. **CVE ID : CVE-2020-4353**	https://www.ibm.com/support/pages/node/6151773	A-IBM-MAAS-010520/67
tririga_application_platform					
Information Exposure	17-04-2020	5	IBM TRIRIGA Application Platform 3.5.3 and 3.6.1 discloses sensitive information in error messages that could aid an attacker formulate	https://www.ibm.com/support/pages/node/6193467	A-IBM-TRIR-010520/68

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			future attacks. IBM X-Force ID: 175993. **CVE ID : CVE-2020-4277**		
spectrum_protect					
Out-of-bounds Write	23-04-2020	10	IBM Spectrum Protect 7.1 and 8.1 server is vulnerable to a stack-based buffer overflow, caused by improper bounds checking. This could allow a remote attacker to execute arbitrary code on the system with the privileges of an administrator or user associated with the Spectrum Protect server or cause the Spectrum Protect server to crash. IBM X-Force ID: 179990. **CVE ID : CVE-2020-4415**	https://www.ibm.com/support/pages/node/6195706	A-IBM-SPEC-010520/69
mq					
Information Exposure	16-04-2020	2.1	IBM MQ 9.1.4 could allow a local attacker to obtain sensitive information by inclusion of sensitive data within runmqras data. IBM X-Force ID: 177937. **CVE ID : CVE-2020-4338**	https://www.ibm.com/support/pages/node/6172539	A-IBM-MQ-010520/70
infosphere_information_server					
Improper Privilege Management	16-04-2020	7.5	IBM InfoSphere Information Server 11.3, 11.5, and 11.7 could be subject to attacks based on privilege escalation due to inappropriate file permissions for files used by WebSphere	https://www.ibm.com/support/pages/node/6191679	A-IBM-INFO-010520/71

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Application Server Network Deployment. IBM X-Force ID: 178412. **CVE ID : CVE-2020-4347**		
idea.me					
paypal-adaptive					
N/A	23-04-2020	5	paypal-adaptive through 0.4.2 manipulation of JavaScript objects resulting in Prototype Pollution. The PayPal function could be tricked into adding or modifying properties of Object.prototype using a __proto__ payload. **CVE ID : CVE-2020-7643**	N/A	A-IDE-PAYP-010520/72
Infradead					
openconnect					
Improper Input Validation	23-04-2020	4.3	OpenConnect through 8.08 mishandles negative return values from X509_check_ function calls, which might assist attackers in performing man-in-the-middle attacks. **CVE ID : CVE-2020-12105**	N/A	A-INF-OPEN-010520/73
Jenkins					
copr					
Cleartext Storage of Sensitive Information	16-04-2020	4	Jenkins Copr Plugin 0.3 and earlier stores credentials unencrypted in job config.xml files on the Jenkins master where they can be viewed by	https://jenkins.io/security/advisory/2020-04-16/#SECURITY-1556	A-JEN-COPR-010520/74

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			users with Extended Read permission, or access to the master file system. **CVE ID : CVE-2020-2177**		
parasoft_findings					
Improper Restriction of XML External Entity Reference ('XXE')	16-04-2020	5.5	Jenkins Parasoft Findings Plugin 10.4.3 and earlier does not configure its XML parser to prevent XML external entity (XXE) attacks. **CVE ID : CVE-2020-2178**	https://jenkins.io/security/advisory/2020-04-16/#SECURITY-1753	A-JEN-PARA-010520/75
yaml_axis					
Deserialization of Untrusted Data	16-04-2020	6.5	Jenkins Yaml Axis Plugin 0.2.0 and earlier does not configure its YAML parser to prevent the instantiation of arbitrary types, resulting in a remote code execution vulnerability. **CVE ID : CVE-2020-2179**	https://jenkins.io/security/advisory/2020-04-16/#SECURITY-1825	A-JEN-YAML-010520/76
amazon_web_services_serverless_application_model					
Deserialization of Untrusted Data	16-04-2020	6.5	Jenkins AWS SAM Plugin 1.2.2 and earlier does not configure its YAML parser to prevent the instantiation of arbitrary types, resulting in a remote code execution vulnerability. **CVE ID : CVE-2020-2180**	https://jenkins.io/security/advisory/2020-04-16/#SECURITY-1736	A-JEN-AMAZ-010520/77
Jetbrains					
youtrack					
Incorrect Default Permissions	22-04-2020	4	In JetBrains YouTrack before 2020.1.659, DB export was accessible to	https://blog.jetbrains.com/blog/202	A-JET-YOUT-010520/78

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			read-only administrators. **CVE ID : CVE-2020-11692**	0/04/22/jetbrains-security-bulletin-q1-2020/	
Improper Input Validation	22-04-2020	5	JetBrains YouTrack before 2020.1.659 was vulnerable to DoS that could be caused by attaching a malformed TIFF file to an issue. **CVE ID : CVE-2020-11693**	https://blog.jetbrains.com/blog/2020/04/22/jetbrains-security-bulletin-q1-2020/	A-JET-YOUT-010520/79
intellij_idea					
N/A	22-04-2020	7.5	In JetBrains IntelliJ IDEA before 2020.1, the license server could be resolved to an untrusted host in some cases. **CVE ID : CVE-2020-11690**	https://blog.jetbrains.com/blog/2020/04/22/jetbrains-security-bulletin-q1-2020/	A-JET-INTE-010520/80
space					
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	22-04-2020	3.5	JetBrains Space through 2020-04-22 allows stored XSS in Chats. **CVE ID : CVE-2020-11416**	https://blog.jetbrains.com/blog/2020/04/22/jetbrains-security-bulletin-q1-2020/	A-JET-SPAC-010520/81
Insufficient Session Expiration	22-04-2020	5	In JetBrains Space through 2020-04-22, the session timeout period was configured improperly. **CVE ID : CVE-2020-11795**	https://blog.jetbrains.com/blog/2020/04/22/jetbrains-security-bulletin-q1-2020/	A-JET-SPAC-010520/82

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Improper Authentication	22-04-2020	7.5	In JetBrains Space through 2020-04-22, the password authentication implementation was insecure. **CVE ID : CVE-2020-11796**	https://blog.jetbrains.com/blog/2020/04/22/jetbrains-security-bulletin-q1-2020/	A-JET-SPAC-010520/83
goland					
Missing Encryption of Sensitive Data	22-04-2020	5	In JetBrains GoLand before 2019.3.2, the plugin repository was accessed via HTTP instead of HTTPS. **CVE ID : CVE-2020-11685**	https://blog.jetbrains.com/blog/2020/04/22/jetbrains-security-bulletin-q1-2020/	A-JET-GOLA-010520/84
teamcity					
Information Exposure	22-04-2020	4	In JetBrains TeamCity before 2019.1.4, a project administrator was able to retrieve some TeamCity server settings. **CVE ID : CVE-2020-11686**	https://blog.jetbrains.com/blog/2020/04/22/jetbrains-security-bulletin-q1-2020/	A-JET-TEAM-010520/85
Information Exposure	22-04-2020	5	In JetBrains TeamCity before 2019.2.2, password values were shown in an unmasked format on several pages. **CVE ID : CVE-2020-11687**	https://blog.jetbrains.com/blog/2020/04/22/jetbrains-security-bulletin-q1-2020/	A-JET-TEAM-010520/86
Insufficient Session Expiration	22-04-2020	5	In JetBrains TeamCity before 2019.2.1, the application state is kept alive after a user ends his session.	https://blog.jetbrains.com/blog/2020/04/22/jetbrains-	A-JET-TEAM-010520/87

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2020-11688	security-bulletin-q1-2020/	
Incorrect Default Permissions	22-04-2020	4	In JetBrains TeamCity before 2019.2.1, a user without appropriate permissions was able to import settings from the settings.kts file. **CVE ID : CVE-2020-11689**	https://blog.jetbrains.com/blog/2020/04/22/jetbrains-security-bulletin-q1-2020/	A-JET-TEAM-010520/88
Information Exposure	22-04-2020	4	In JetBrains TeamCity 2018.2 through 2019.2.1, a project administrator was able to see scrambled password parameters used in a project. The issue was resolved in 2019.2.2. **CVE ID : CVE-2020-11938**	https://blog.jetbrains.com/blog/2020/04/22/jetbrains-security-bulletin-q1-2020/	A-JET-TEAM-010520/89
Jitsi					
meet					
Use of Hard-coded Credentials	17-04-2020	7.5	The Jitsi Meet (aka docker-jitsi-meet) stack on Docker before stable-4384-1 uses default passwords (such as passw0rd) for system accounts. **CVE ID : CVE-2020-11878**	https://github.com/jitsi/docker-jitsi-meet/blob/master/CHANGELOG.md#stable-4384-1	A-JIT-MEET-010520/90
Joomla					
joomla\!					
Incorrect Authorization	21-04-2020	5	An issue was discovered in Joomla! before 3.9.17. Incorrect ACL checks in the access level section of	N/A	A-JOO-JOOM-010520/91

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			com_users allow the unauthorized deletion of usergroups. **CVE ID : CVE-2020-11889**		
Improper Input Validation	21-04-2020	5	An issue was discovered in Joomla! before 3.9.17. Improper input validations in the usergroup table class could lead to a broken ACL configuration. **CVE ID : CVE-2020-11890**	N/A	A-JOO-JOOM-010520/92
Incorrect Authorization	21-04-2020	5	An issue was discovered in Joomla! before 3.9.17. Incorrect ACL checks in the access level section of com_users allow the unauthorized editing of usergroups. **CVE ID : CVE-2020-11891**	N/A	A-JOO-JOOM-010520/93
KDE					
kmail					
N/A	17-04-2020	6.4	An issue was discovered in KDE KMail before 19.12.3. By using the proprietary (non-RFC6068) "mailto?attach=..." parameter, a website (or other source of mailto links) can make KMail attach local files to a composed email message without showing a warning to the user, as demonstrated by an	N/A	A-KDE-KMAI-010520/94

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			attach=.bash_history value. **CVE ID : CVE-2020-11880**		
Libming					
libming					
Out-of-bounds Read	19-04-2020	6.4	Ming (aka libming) 0.4.8 has a heap-based buffer over-read (8 bytes) in the function decompileIF() in decompile.c. **CVE ID : CVE-2020-11894**	N/A	A-LIB-LIBM-010520/95
Out-of-bounds Read	19-04-2020	6.4	Ming (aka libming) 0.4.8 has a heap-based buffer over-read (2 bytes) in the function decompileIF() in decompile.c. **CVE ID : CVE-2020-11895**	N/A	A-LIB-LIBM-010520/96
libslirp_project					
libslirp					
Use After Free	22-04-2020	5	A use after free vulnerability in ip_reass() in ip_input.c of libslirp 4.2.0 and prior releases allows crafted packets to cause a denial of service. **CVE ID : CVE-2020-1983**	N/A	A-LIB-LIBS-010520/97
Linuxfoundation					
ceph					
NULL Pointer Dereference	22-04-2020	5	An issue was discovered in Ceph through 13.2.9. A POST request with an invalid tagging XML can crash the RGW process by triggering a NULL pointer	N/A	A-LIN-CEPH-010520/98

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			exception. **CVE ID : CVE-2020-12059**		
Improper Limitation of a Pathname to a Restricted Directory ('Path Traversal')	21-04-2020	5	A path traversal flaw was found in the Ceph dashboard implemented in upstream versions v14.2.5, v14.2.6, v15.0.0 of Ceph storage and has been fixed in versions 14.2.7 and 15.1.0. An unauthenticated attacker could use this flaw to cause information disclosure on the host machine running the Ceph dashboard. **CVE ID : CVE-2020-1699**	https://bugzilla.redhat.com/show_bug.cgi?id=CVE-2020-1699	A-LIN-CEPH-010520/99
mappresspro					
mappress					
Unrestricted Upload of File with Dangerous Type	23-04-2020	6.5	The mappress-google-maps-for-wordpress plugin before 2.53.9 for WordPress does not correctly implement AJAX functions with nonces (or capability checks), leading to remote code execution. **CVE ID : CVE-2020-12077**	N/A	A-MAP-MAPP-010520/100
media_library_assistant_project					
media_library_assistant					
Improper Neutralization of Special Elements in Output Used by a Downstream	20-04-2020	7.5	In the media-library-assistant plugin before 2.82 for WordPress, Remote Code Execution can occur via the tax_query, meta_query, or	N/A	A-MED-MEDI-010520/101

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Component ('Injection')			date_query parameter in mla_gallery via an admin. **CVE ID : CVE-2020-11928**		
Mediawiki					
mediawiki					
Information Exposure	21-04-2020	5	The CentralAuth extension through REL1_34 for MediaWiki allows remote attackers to obtain sensitive hidden account information via an api.php?action=query&meta=globaluserinfo&guiuser= request. In other words, the information can be retrieved via the action API even though access would be denied when simply visiting wiki/Special:CentralAuth in a web browser. **CVE ID : CVE-2020-12051**	N/A	A-MED-MEDI-010520/102
Microfocus					
enterprise_developer					
Insufficiently Protected Credentials	17-04-2020	6.5	Insufficiently protected credentials vulnerability on Micro Focus enterprise developer and enterprise server, affecting all version prior to 4.0 Patch Update 16, and version 5.0 Patch Update 6. The vulnerability could allow an attacker to transmit hashed credentials for the user account running the	N/A	A-MIC-ENTE-010520/103

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Micro Focus Directory Server (MFDS) to an arbitrary site, compromising that account's security. **CVE ID : CVE-2020-9523**		
enterprise_server					
Insufficiently Protected Credentials	17-04-2020	6.5	Insufficiently protected credentials vulnerability on Micro Focus enterprise developer and enterprise server, affecting all version prior to 4.0 Patch Update 16, and version 5.0 Patch Update 6. The vulnerability could allow an attacker to transmit hashed credentials for the user account running the Micro Focus Directory Server (MFDS) to an arbitrary site, compromising that account's security. **CVE ID : CVE-2020-9523**	N/A	A-MIC-ENTE-010520/104
Mitel					
mivoice_connect					
Improper Input Validation	17-04-2020	7.5	A remote code execution vulnerability in UCB component of Mitel MiVoice Connect before 19.1 SP1 could allow an unauthenticated remote attacker to execute arbitrary scripts due to insufficient validation of URL parameters. A successful exploit could allow an attacker to gain	https://www.mitel.com/support/security-advisories/mitel-product-security-advisory-20-0004	A-MIT-MIVO-010520/105

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			access to sensitive information. **CVE ID : CVE-2020-10211**		
Inadequate Encryption Strength	17-04-2020	5	A weak encryption vulnerability in Mitel MiVoice Connect Client before 214.100.1214.0 could allow an unauthenticated attacker to gain access to user credentials. A successful exploit could allow an attacker to access the system with compromised user credentials. **CVE ID : CVE-2020-10377**	https://www.mitel.com/support/security-advisories/mitel-product-security-advisory-20-0004	A-MIT-MIVO-010520/106
mivoice_connect_client					
Improper Input Validation	17-04-2020	7.5	A remote code execution vulnerability in UCB component of Mitel MiVoice Connect before 19.1 SP1 could allow an unauthenticated remote attacker to execute arbitrary scripts due to insufficient validation of URL parameters. A successful exploit could allow an attacker to gain access to sensitive information. **CVE ID : CVE-2020-10211**	https://www.mitel.com/support/security-advisories/mitel-product-security-advisory-20-0004	A-MIT-MIVO-010520/107
Inadequate Encryption Strength	17-04-2020	5	A weak encryption vulnerability in Mitel MiVoice Connect Client	https://www.mitel.com/support/sec	A-MIT-MIVO-010520/108

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			before 214.100.1214.0 could allow an unauthenticated attacker to gain access to user credentials. A successful exploit could allow an attacker to access the system with compromised user credentials. **CVE ID : CVE-2020-10377**	urity-advisories/mitel-product-security-advisory-20-0004	
Mongodb					
c_driver					
Integer Overflow or Wraparound	24-04-2020	4.3	bson before 0.8 incorrectly uses int rather than size_t for many variables, parameters, and return values. In particular, the bson_ensure_space() parameter bytesNeeded could have an integer overflow via properly constructed bson input. **CVE ID : CVE-2020-12135**	N/A	A-MON-C_DR-010520/109
msi					
true_color					
Unquoted Search Path or Element	21-04-2020	10	Unquoted search path vulnerability in MSI True Color before 3.0.52.0 allows privilege escalation to SYSTEM. **CVE ID : CVE-2020-8842**	N/A	A-MSI-TRUE-010520/110
Netapp					
data_ontap					

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Uncontrolled Resource Consumption	17-04-2020	5	ntpd in ntp before 4.2.8p14 and 4.3.x before 4.3.100 allows an off-path attacker to block unauthenticated synchronization via a server mode packet with a spoofed source IP address, because transmissions are rescheduled even when a packet lacks a valid origin timestamp. **CVE ID : CVE-2020-11868**	https://security.netapp.com/advisory/ntap-20200424-0002/	A-NET-DATA-010520/111
NTP					
ntp					
Uncontrolled Resource Consumption	17-04-2020	5	ntpd in ntp before 4.2.8p14 and 4.3.x before 4.3.100 allows an off-path attacker to block unauthenticated synchronization via a server mode packet with a spoofed source IP address, because transmissions are rescheduled even when a packet lacks a valid origin timestamp. **CVE ID : CVE-2020-11868**	https://security.netapp.com/advisory/ntap-20200424-0002/	A-NTP-NTP-010520/112
opcfoundation					
unified_architecture_.net-standard					
Insufficient Session Expiration	22-04-2020	5	This vulnerability allows remote attackers to create a denial-of-service condition on affected installations of OPC	N/A	A-OPC-UNIF-010520/113

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Foundation UA .NET Standard 1.04.358.30. Authentication is not required to exploit this vulnerability. The specific flaw exists within the handling of sessions. The issue results from the lack of proper locking when performing operations on an object. An attacker can leverage this vulnerability to create a denial-of-service condition against the application. Was ZDI-CAN-10295. **CVE ID : CVE-2020-8867**		
Openmrs					
openmrs					
Improper Input Validation	17-04-2020	4.3	OpenMRS 2.9 and prior copies "Referrer" header values into an html element named "redirectUrl" within many webpages (such as login.htm). There is insufficient validation for this parameter, which allows for the possibility of cross-site scripting. **CVE ID : CVE-2020-5728**	N/A	A-OPE-OPEN-010520/114
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	17-04-2020	4.3	In OpenMRS 2.9 and prior, the UI Framework Error Page reflects arbitrary, user-supplied input back to the browser, which can result in XSS. Any page that is able to trigger a UI Framework	N/A	A-OPE-OPEN-010520/115

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Error is susceptible to this issue. **CVE ID : CVE-2020-5729**		
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	17-04-2020	4.3	In OpenMRS 2.9 and prior, the sessionLocation parameter for the login page is vulnerable to cross-site scripting. **CVE ID : CVE-2020-5730**	N/A	A-OPE-OPEN-010520/116
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	17-04-2020	4.3	In OpenMRS 2.9 and prior, the app parameter for the ActiveVisit's page is vulnerable to cross-site scripting. **CVE ID : CVE-2020-5731**	N/A	A-OPE-OPEN-010520/117
URL Redirection to Untrusted Site ('Open Redirect')	17-04-2020	5.8	In OpenMRS 2.9 and prior, he import functionality of the Data Exchange Module does not properly redirect to a login page when an unauthenticated user attempts to access it. This allows unauthenticated users to use a feature typically restricted to administrators. **CVE ID : CVE-2020-5732**	N/A	A-OPE-OPEN-010520/118
URL Redirection to Untrusted Site ('Open Redirect')	17-04-2020	5.8	In OpenMRS 2.9 and prior, the export functionality of the Data Exchange Module does not properly redirect to a login page when an unauthenticated user attempts to access it. This allows the export of	N/A	A-OPE-OPEN-010520/119

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			potentially sensitive information. **CVE ID : CVE-2020-5733**		
phproject					
phproject					
Unrestricted Upload of File with Dangerous Type	22-04-2020	6.5	In Phproject before version 1.7.8, there's a vulnerability which allows users with access to file uploads to execute arbitrary code. This is patched in version 1.7.8. **CVE ID : CVE-2020-11011**	https://github.com/Alanaktion/phproject/security/advisories/GHSA-4j97-6w6q-gxjx	A-PHP-PHPR-010520/120
Plex					
plex_media_server					
Improper Input Validation	22-04-2020	7.2	Improper Input Validation in Plex Media Server on Windows allows a local, unauthenticated attacker to execute arbitrary Python code with SYSTEM privileges. **CVE ID : CVE-2020-5740**	https://www.tenable.com/security/research/tra-2020-25	A-PLE-PLEX-010520/121
Prestashop					
prestashop_link					
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	16-04-2020	3.5	In the ps_link module for PrestaShop before version 3.1.0, there is a stored XSS when you create or edit a link list block with the title field. The problem is fixed in 3.1.0 **CVE ID : CVE-2020-5266**	https://github.com/PrestaShop/ps_linklist/security/advisories/GHSA-vr7g-vqp5-966j	A-PRE-PRES-010520/122

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
prestashop_linklist					
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	16-04-2020	3.5	In PrestaShop module ps_linklist versions before 3.1.0, there is a stored XSS when using custom URLs. The problem is fixed in version 3.1.0 **CVE ID : CVE-2020-5273**	https://github.com/PrestaShop/ps_linklist/security/advisories/GHSA-cx2r-mf6x-55rx	A-PRE-PRES-010520/123
prestashop_socialfollow					
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	16-04-2020	3.5	PrestaShop module ps_facetedsearch versions before 2.1.0 has a reflected XSS with social networks fields The problem is fixed in 2.1.0 **CVE ID : CVE-2020-5294**	https://github.com/PrestaShop/ps_socialfollow/security/advisories/GHSA-774w-fg8p-7c8w	A-PRE-PRES-010520/124
prestashop					
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	20-04-2020	4.3	In PrestaShop between versions 1.7.6.0 and 1.7.6.5, there is a reflected XSS with `back` parameter. The problem is fixed in 1.7.6.5 **CVE ID : CVE-2020-5285**	https://github.com/PrestaShop/PrestaShop/security/advisories/GHSA-j3r6-33hf-m8wh	A-PRE-PRES-010520/125
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	20-04-2020	4.3	In PrestaShop between versions 1.7.4.0 and 1.7.6.5, there is a reflected XSS when uploading a wrong file. The problem is fixed in 1.7.6.5 **CVE ID : CVE-2020-5286**	https://github.com/PrestaShop/PrestaShop/security/advisories/GHSA-98j8-hvjv-x47j	A-PRE-PRES-010520/126
Incorrect Authorization	20-04-2020	6.4	In PrestaShop between versions 1.5.5.0 and 1.7.6.5, there is improper access control on customers search. The problem is fixed in 1.7.6.5.	https://github.com/PrestaShop/PrestaShop/security/advisories/GHSA-r6rp-	A-PRE-PRES-010520/127

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2020-5287	6gv6-r9hq	
Incorrect Authorization	20-04-2020	6.4	"In PrestaShop between versions 1.7.0.0 and 1.7.6.5, there is improper access controls on product attributes page. The problem is fixed in 1.7.6.5. **CVE ID : CVE-2020-5288**	https://github.com/PrestaShop/PrestaShop/security/advisories/GHSA-4wxg-33h3-3w5r	A-PRE-PRES-010520/128
Incorrect Authorization	20-04-2020	6.4	In PrestaShop between versions 1.7.0.0 and 1.7.6.5, there are improper access controls on product page with combinations, attachments and specific prices. The problem is fixed in 1.7.6.5. **CVE ID : CVE-2020-5293**	https://github.com/PrestaShop/PrestaShop/security/advisories/GHSA-cvjj-grfv-f56w	A-PRE-PRES-010520/129
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	20-04-2020	4.3	In PrestaShop before version 1.7.6.5, there is a reflected XSS while running the security compromised page. It allows anyone to execute arbitrary action. The problem is patched in the 1.7.6.5. **CVE ID : CVE-2020-5264**	https://github.com/PrestaShop/PrestaShop/commit/06b7765c91c58e09ab4f8ddafbde02070fcb6f3a, https://github.com/PrestaShop/PrestaShop/security/advisories/GHSA-48vj-vvr6-jj4f	A-PRE-PRES-010520/130
Improper Neutralization of Input During Web Page Generation	20-04-2020	4.3	In PrestaShop between versions 1.7.6.1 and 1.7.6.5, there is a reflected XSS on AdminAttributesGroups	https://github.com/PrestaShop/PrestaShop/security/advisories	A-PRE-PRES-010520/131

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
('Cross-site Scripting')			page. The problem is patched in 1.7.6.5. **CVE ID : CVE-2020-5265**	/GHSA-7fmr-5vcc-329j	
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	20-04-2020	4.3	In PrestaShop between versions 1.7.6.1 and 1.7.6.5, there is a reflected XSS on AdminFeatures page by using the `id_feature` parameter. The problem is fixed in 1.7.6.5 **CVE ID : CVE-2020-5269**	https://github.com/PrestaShop/PrestaShop/security/advisories/GHSA-87jh-7xpg-6v93	A-PRE-PRES-010520/132
URL Redirection to Untrusted Site ('Open Redirect')	20-04-2020	5.8	In PrestaShop between versions 1.7.6.0 and 1.7.6.5, there is an open redirection when using back parameter. The impacts can be many, and vary from the theft of information and credentials to the redirection to malicious websites containing attacker-controlled content, which in some cases even cause XSS attacks. So even though an open redirection might sound harmless at first, the impacts of it can be severe should it be exploitable. The problem is fixed in 1.7.6.5 **CVE ID : CVE-2020-5270**	https://github.com/PrestaShop/PrestaShop/security/advisories/GHSA-375w-q56h-h7qc	A-PRE-PRES-010520/133
Improper Neutralization of Input During Web Page Generation	20-04-2020	4.3	In PrestaShop between versions 1.6.0.0 and 1.7.6.5, there is a reflected XSS with `date_from` and `date_to` parameters in	https://github.com/PrestaShop/PrestaShop/security/advisories	A-PRE-PRES-010520/134

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
('Cross-site Scripting')			the dashboard page This problem is fixed in 1.7.6.5 **CVE ID : CVE-2020-5271**	/GHSA-m2x6-c2c6-pjrx	
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	20-04-2020	4.3	In PrestaShop between versions 1.5.5.0 and 1.7.6.5, there is a reflected XSS on Search page with `alias` and `search` parameters. The problem is patched in 1.7.6.5 **CVE ID : CVE-2020-5272**	https://github.com/PrestaShop/PrestaShop/security/advisories/GHSA-rpg3-f23r-jmqv	A-PRE-PRES-010520/135
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	20-04-2020	4.3	In PrestaShop between versions 1.7.1.0 and 1.7.6.5, there is a reflected XSS on AdminCarts page with `cartBox` parameter The problem is fixed in 1.7.6.5 **CVE ID : CVE-2020-5276**	https://github.com/PrestaShop/PrestaShop/security/advisories/GHSA-q6pr-42v5-v97q	A-PRE-PRES-010520/136
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	20-04-2020	4.3	In PrestaShop between versions 1.5.4.0 and 1.7.6.5, there is a reflected XSS on Exception page The problem is fixed in 1.7.6.5 **CVE ID : CVE-2020-5278**	https://github.com/PrestaShop/PrestaShop/security/advisories/GHSA-mrpj-67mq-3fr5	A-PRE-PRES-010520/137
Incorrect Authorization	20-04-2020	6.4	In PrestaShop between versions 1.5.0.0 and 1.7.6.5, there are improper access control since the the version 1.5.0.0 for legacy controllers. - admin-dev/index.php/configure/shop/customer-preferences/ - admin-dev/index.php/improve/international/translations/ - admin-	https://github.com/PrestaShop/PrestaShop/security/advisories/GHSA-74vp-ww64-w2gm	A-PRE-PRES-010520/138

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			dev/index.php/improve/international/geolocation/ - admin-dev/index.php/improve/international/localization - admin-dev/index.php/configure/advanced/performance - admin-dev/index.php/sell/orders/delivery-slips/ - admin-dev/index.php?controller=AdminStatuses The problem is fixed in 1.7.6.5 **CVE ID : CVE-2020-5279**		
python-markdown2_project					
python-markdown2					
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	20-04-2020	4.3	python-markdown2 through 2.3.8 allows XSS because element names are mishandled unless a \w+ match succeeds. For example, an attack might use elementname@ or elementname- with an onclick attribute. **CVE ID : CVE-2020-11888**	N/A	A-PYT-PYTH-010520/139
Qdpm					
qdpm					
Unrestricted Upload of File with Dangerous Type	16-04-2020	10	In qdPM 9.1, an attacker can upload a malicious .php file to the server by exploiting the Add Profile Photo capability with a crafted content-type value. After that, the attacker can execute an arbitrary command on the	N/A	A-QDP-QDPM-010520/140

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			server using this malicious file. **CVE ID : CVE-2020-11811**		
Improper Neutralization of Special Elements in Output Used by a Downstream Component ('Injection')	16-04-2020	5.8	A Host Header Injection vulnerability in qdPM 9.1 may allow an attacker to spoof a particular header and redirect users to malicious websites. **CVE ID : CVE-2020-11814**	N/A	A-QDP-QDPM-010520/141
QT					
qt					
Use After Free	27-04-2020	7.5	setMarkdown in Qt before 5.14.2 has a use-after-free related to QTextMarkdownImporter::insertBlock. **CVE ID : CVE-2020-12267**	N/A	A-QT-QT-010520/142
re2c					
re2c					
Out-of-bounds Write	21-04-2020	6.8	re2c 1.3 has a heap-based buffer overflow in Scanner::fill in parse/scanner.cc via a long lexeme. **CVE ID : CVE-2020-11958**	N/A	A-RE2-RE2C-010520/143
Redhat					
ceph_storage					
Improper Limitation of a Pathname to a Restricted Directory	21-04-2020	5	A path traversal flaw was found in the Ceph dashboard implemented in upstream versions v14.2.5, v14.2.6, v15.0.0	https://bugzilla.redhat.com/show_bug.cgi?id=CVE-	A-RED-CEPH-010520/144

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
('Path Traversal')			of Ceph storage and has been fixed in versions 14.2.7 and 15.1.0. An unauthenticated attacker could use this flaw to cause information disclosure on the host machine running the Ceph dashboard. **CVE ID : CVE-2020-1699**	2020-1699	
rukovoditel					
rukovoditel					
Improper Neutralization of Special Elements used in an SQL Command ('SQL Injection')	16-04-2020	7.5	Rukovoditel 2.5.2 is affected by a SQL injection vulnerability because of improper handling of the filters[0][value] or filters[1][value] parameter. **CVE ID : CVE-2020-11812**	N/A	A-RUK-RUKO-010520/145
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	16-04-2020	3.5	In Rukovoditel 2.5.2, there is a stored XSS vulnerability on the configuration page via the copyright text input. Thus, an attacker can inject a malicious script to steal all users' valuable data. This copyright text is on every page so this attack vector can be very dangerous. **CVE ID : CVE-2020-11813**	N/A	A-RUK-RUKO-010520/146
Unrestricted Upload of File with Dangerous	16-04-2020	6.8	In Rukovoditel 2.5.2, attackers can upload arbitrary file to the server by just changing the	N/A	A-RUK-RUKO-010520/147

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Type			content-type value. As a result of that, an attacker can execute a command on the server. This specific attack only occurs without the Maintenance Mode setting. **CVE ID : CVE-2020-11815**		
Improper Neutralization of Special Elements used in an SQL Command ('SQL Injection')	16-04-2020	7.5	Rukovoditel 2.5.2 is affected by a SQL injection vulnerability because of improper handling of the reports_id (POST) parameter. **CVE ID : CVE-2020-11816**	N/A	A-RUK-RUKO-010520/148
Cross-Site Request Forgery (CSRF)	16-04-2020	6.8	In Rukovoditel 2.5.2 has a form_session_token value to prevent CSRF attacks. This protection mechanism can be bypassed with another user's valid token. Thus, an attacker can change the Admin password by using a CSRF attack and escalate his/her privileges. **CVE ID : CVE-2020-11818**	N/A	A-RUK-RUKO-010520/149
Improper Input Validation	16-04-2020	7.5	In Rukovoditel 2.5.2, an attacker may inject an arbitrary .php file location instead of a language file and thus achieve command execution. **CVE ID : CVE-2020-11819**	N/A	A-RUK-RUKO-010520/150

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Improper Neutralization of Special Elements used in an SQL Command ('SQL Injection')	16-04-2020	7.5	Rukovoditel 2.5.2 is affected by a SQL injection vulnerability because of improper handling of the entities_id parameter. **CVE ID : CVE-2020-11820**	N/A	A-RUK-RUKO-010520/151
se					
tristation_1131					
Information Exposure	16-04-2020	5	**VERSION NOT SUPPORTED WHEN ASSIGNED** A vulnerability could cause certain data to be visible on the network when the 'password' feature is enabled. This vulnerability was discovered in and remediated in versions v4.9.1 and v4.10.1 on May 30, 2013. The 'password' feature is an additional optional check performed by TS1131 that it is connected to a specific controller. This data is sent as clear text and is visible on the network. This feature is not present in TriStation 1131 versions v4.9.1 and v4.10.1 through current. Therefore, the vulnerability is not present in these versions. **CVE ID : CVE-2020-7483**	N/A	A-SE-TRIS-010520/152
N/A	16-04-2020	4.3	**VERSION NOT SUPPORTED WHEN	N/A	A-SE-TRIS-

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			ASSIGNED** A vulnerability with the former 'password' feature could allow a denial of service attack if the user is not following documented guidelines pertaining to dedicated TriStation connection and key-switch protection. This vulnerability was discovered and remediated in versions v4.9.1 and v4.10.1 on May 30, 2013. This feature is not present in version v4.9.1 and v4.10.1 through current. Therefore, the vulnerability is not present in these versions. **CVE ID : CVE-2020-7484**		010520/153
N/A	16-04-2020	7.5	**VERSION NOT SUPPORTED WHEN ASSIGNED** A legacy support account in the TriStation software version v4.9.0 and earlier could cause improper access to the TriStation host machine. This was addressed in TriStation version v4.9.1 and v4.10.1 released on May 30, 2013.1 **CVE ID : CVE-2020-7485**	N/A	A-SE-TRIS-010520/154
ecostruxure_machine_expert					
Insufficient Verification of Data	22-04-2020	7.5	A CWE-345: Insufficient Verification of Data Authenticity vulnerability	N/A	A-SE-ECOS-010520/155

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Authenticity			exists which could allow the attacker to execute malicious code on the Modicon M218, M241, M251, and M258 controllers. **CVE ID : CVE-2020-7487**		
Cleartext Transmission of Sensitive Information	22-04-2020	5	A CWE-319: Cleartext Transmission of Sensitive Information vulnerability exists which could leak sensitive information transmitted between the software and the Modicon M218, M241, M251, and M258 controllers. **CVE ID : CVE-2020-7488**	N/A	A-SE-ECOS-010520/156
somachine					
Insufficient Verification of Data Authenticity	22-04-2020	7.5	A CWE-345: Insufficient Verification of Data Authenticity vulnerability exists which could allow the attacker to execute malicious code on the Modicon M218, M241, M251, and M258 controllers. **CVE ID : CVE-2020-7487**	N/A	A-SE-SOMA-010520/157
Cleartext Transmission of Sensitive Information	22-04-2020	5	A CWE-319: Cleartext Transmission of Sensitive Information vulnerability exists which could leak sensitive information transmitted between the software and the Modicon M218, M241, M251, and M258 controllers. **CVE ID : CVE-2020-7488**	N/A	A-SE-SOMA-010520/158

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
somachine_motion					
Insufficient Verification of Data Authenticity	22-04-2020	7.5	A CWE-345: Insufficient Verification of Data Authenticity vulnerability exists which could allow the attacker to execute malicious code on the Modicon M218, M241, M251, and M258 controllers. **CVE ID : CVE-2020-7487**	N/A	A-SE-SOMA-010520/159
Cleartext Transmission of Sensitive Information	22-04-2020	5	A CWE-319: Cleartext Transmission of Sensitive Information vulnerability exists which could leak sensitive information transmitted between the software and the Modicon M218, M241, M251, and M258 controllers. **CVE ID : CVE-2020-7488**	N/A	A-SE-SOMA-010520/160
vijeo_designer					
Untrusted Search Path	22-04-2020	6.9	A CWE-426: Untrusted Search Path vulnerability exists in Vijeo Designer Basic (V1.1 HotFix 15 and prior) and Vijeo Designer (V6.9 SP9 and prior), which could cause arbitrary code execution on the system running Vijeo Basic when a malicious DLL library is loaded by the Product. **CVE ID : CVE-2020-7490**	N/A	A-SE-VIJE-010520/161
Shopizer					
shopizer					
Improper	16-04-2020	4	In Shopizer before	https://githu	A-SHO-

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Input Validation			version 2.11.0, using API or Controller based versions negative quantity is not adequately validated hence creating incorrect shopping cart and order total. This vulnerability makes it possible to create a negative total in the shopping cart. This has been patched in version 2.11.0. **CVE ID : CVE-2020-11007**	b.com/shopizer-ecommerce/shopizer/security/advisories/GHSA-w8rc-pgxq-x2cj	SHOP-010520/162
Simplesamlphp					
simplesamlphp					
Information Exposure	21-04-2020	3.5	SimpleSAMLphp versions before 1.18.6 contain an information disclosure vulnerability. The module controller in `SimpleSAML\Module` that processes requests for pages hosted by modules, has code to identify paths ending with `.php` and process those as PHP code. If no other suitable way of handling the given path exists it presents the file to the browser. The check to identify paths ending with `.php` does not account for uppercase letters. If someone requests a path ending with e.g. `.PHP` and the server is serving the code from a case-	https://github.com/simplesamlphp/simplesamlphp/security/advisories/GHSA-24m3-w8g9-jwpq	A-SIM-SIMP-010520/163

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			insensitive file system, such as on Windows, the processing of the PHP code does not occur, and the source code is instead presented to the browser. An attacker may use this issue to gain access to the source code in third-party modules that is meant to be private, or even sensitive. However, the attack surface is considered small, as the attack will only work when SimpleSAMLphp serves such content from a file system that is not case-sensitive, such as on Windows. This issue is fixed in version 1.18.6. **CVE ID : CVE-2020-5301**		
Sonatype					
nexus_repository_manager_3					
Incorrect Authorization	20-04-2020	6.5	An issue was discovered in Sonatype Nexus Repository Manager in versions 3.21.1 and 3.22.0. It is possible for a user with appropriate privileges to create, modify, and execute scripting tasks without use of the UI or API. NOTE: in 3.22.0, scripting is disabled by default (making this not exploitable). **CVE ID : CVE-2020-**	https://support.sonatype.com/hc/en-us/articles/360046233714	A-SON-NEXU-010520/164

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			11753		
Sophos					
anti-virus_for_sophos_central					
Improper Privilege Management	17-04-2020	6.5	Mac Endpoint for Sophos Central before 9.9.6 and Mac Endpoint for Sophos Home before 2.2.6 allow Privilege Escalation. **CVE ID : CVE-2020-10947**	https://community.sophos.com/b/security-blog/posts/advisory-cve-2020-10947--sophos-anti-virus-for-macos-privilege-escalation	A-SOP-ANTI-010520/165
anti-virus_for_sophos_home					
Improper Privilege Management	17-04-2020	6.5	Mac Endpoint for Sophos Central before 9.9.6 and Mac Endpoint for Sophos Home before 2.2.6 allow Privilege Escalation. **CVE ID : CVE-2020-10947**	https://community.sophos.com/b/security-blog/posts/advisory-cve-2020-10947--sophos-anti-virus-for-macos-privilege-escalation	A-SOP-ANTI-010520/166
supsystic					
data_tables_generator					
Incorrect Default Permissions	23-04-2020	6.5	The data-tables-generator-by-supsystic plugin before 1.9.92 for WordPress lacks capability checks for AJAX actions. **CVE ID : CVE-2020-12075**	N/A	A-SUP-DATA-010520/167

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Cross-Site Request Forgery (CSRF)	23-04-2020	6.8	The data-tables-generator-by-supsystic plugin before 1.9.92 for WordPress lacks CSRF nonce checks for AJAX actions. One consequence of this is stored XSS. **CVE ID : CVE-2020-12076**	N/A	A-SUP-DATA-010520/168
svg2png_project					
svg2png					
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	17-04-2020	4.3	svg2png 4.1.1 allows XSS with resultant SSRF via JavaScript inside an SVG document. **CVE ID : CVE-2020-11887**	N/A	A-SVG-SVG2-010520/169
Sysaid					
on-premise					
Unrestricted Upload of File with Dangerous Type	21-04-2020	10	SysAid On-Premise 20.1.11, by default, allows the AJP protocol port, which is vulnerable to a GhostCat attack. Additionally, it allows unauthenticated access to upload files, which can be used to execute commands on the system by chaining it with a GhostCat attack. **CVE ID : CVE-2020-10569**	N/A	A-SYS-ON-P-010520/170
Tenable					
tenable.sc					
Improper Neutralization	17-04-2020	3.5	Stored XSS in Tenable.Sc before 5.14.0 could allow	N/A	A-TEN-TENA-

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
of Input During Web Page Generation ('Cross-site Scripting')			an authenticated remote attacker to craft a request to execute arbitrary script code in a user's browser session. Updated input validation techniques have been implemented to correct this issue. **CVE ID : CVE-2020-5737**		010520/171
tortoise_orm_project					
tortoise_orm					
Improper Neutralization of Special Elements used in an SQL Command ('SQL Injection')	20-04-2020	6.5	In Tortoise ORM before versions 0.15.23 and 0.16.6, various forms of SQL injection have been found for MySQL and when filtering or doing mass-updates on char/text fields. SQLite & PostgreSQL are only affected when filtering with contains, starts_with, or ends_with filters (and their case-insensitive counterparts). **CVE ID : CVE-2020-11010**	https://github.com/tortoise/tortoise-orm/security/advisories/GHSA-9j2c-x8qm-qmjq	A-TOR-TORT-010520/172
Vestacp					
vesta_control_panel					
Improper Input Validation	21-04-2020	9	A remote command execution in Vesta Control Panel through 0.9.8-26 allows any authenticated user to execute arbitrary commands on the system via cron jobs. **CVE ID : CVE-2020-10786**	N/A	A-VES-VEST-010520/173

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Improper Privilege Management	21-04-2020	9	An elevation of privilege in Vesta Control Panel through 0.9.8-26 allows an attacker to gain root system access from the admin account via v-change-user-password (aka the user password change script). **CVE ID : CVE-2020-10787**	N/A	A-VES-VEST-010520/174
Vmware					
installbuilder					
Uncontrolled Resource Consumption	20-04-2020	5	InstallBuilder AutoUpdate tool and regular installers enabling <checkForUpdates> built with versions earlier than 19.11 are vulnerable to Billion laughs attack (denial-of-service). **CVE ID : CVE-2020-3946**	https://blog.installbuilder.com/2019/12/configure-autoupdate-project-settings.html	A-VMW-INST-010520/175
Webkitgtk					
webkitgtk					
Use After Free	17-04-2020	7.5	A use-after-free issue exists in WebKitGTK before 2.28.1 and WPE WebKit before 2.28.1 via crafted web content that allows remote attackers to execute arbitrary code or cause a denial of service (memory corruption and application crash). **CVE ID : CVE-2020-11793**	https://webkitgtk.org/security/WSA-2020-0004.html, https://wpewebkit.org/security/WSA-2020-0004.html	A-WEB-WEBK-010520/176
webtoffee					

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
import_export_wordpress_users					
Improper Neutralization of Special Elements in Output Used by a Downstream Component ('Injection')	23-04-2020	6.5	The users-customers-import-export-for-wp-woocommerce plugin before 1.3.9 for WordPress allows subscribers to import administrative accounts via CSV. **CVE ID : CVE-2020-12074**	N/A	A-WEB-IMPO-010520/177
whoopsie_project					
whoopsie					
Integer Overflow or Wraparound	24-04-2020	4.3	bson before 0.8 incorrectly uses int rather than size_t for many variables, parameters, and return values. In particular, the bson_ensure_space() parameter bytesNeeded could have an integer overflow via properly constructed bson input. **CVE ID : CVE-2020-12135**	N/A	A-WHO-WHOO-010520/178
wpewebkit					
wpe_webkit					
Use After Free	17-04-2020	7.5	A use-after-free issue exists in WebKitGTK before 2.28.1 and WPE WebKit before 2.28.1 via crafted web content that allows remote attackers to execute arbitrary code or cause a denial of service (memory corruption and	https://webkitgtk.org/security/WSA-2020-0004.html, https://wpewebkit.org/security/WSA-2020-0004.html	A-WPE-WPE_-010520/179

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			application crash). **CVE ID : CVE-2020-11793**		
Wso2					
enterprise_integrator					
Improper Restriction of XML External Entity Reference ('XXE')	17-04-2020	6.5	WSO2 Enterprise Integrator through 6.6.0 has an XXE vulnerability where a user (with admin console access) can use the XML validator to make unintended network invocations such as SSRF via an uploaded file. **CVE ID : CVE-2020-11885**	N/A	A-WSO-ENTE-010520/180
Zohocorp					
manageengine_opmanager					
Information Exposure	20-04-2020	5	Zoho ManageEngine OpManager before 125120 allows an unauthenticated user to retrieve an API key via a servlet call. **CVE ID : CVE-2020-11946**	N/A	A-ZOH-MANA-010520/181
Zoom					
meetings					
Use of Hard-coded Credentials	17-04-2020	5	airhost.exe in Zoom Client for Meetings 4.6.11 uses the SHA-256 hash of 0123425234234fsdfsdr3242 for initialization of an OpenSSL EVP AES-256 CBC context. **CVE ID : CVE-2020-11876**	N/A	A-ZOO-MEET-010520/182

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Inadequate Encryption Strength	17-04-2020	5	airhost.exe in Zoom Client for Meetings 4.6.11 uses 3423423432325249 as the Initialization Vector (IV) for AES-256 CBC encryption. **CVE ID : CVE-2020-11877**	N/A	A-ZOO-MEET-010520/183
Zulip					
zulip_server					
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	20-04-2020	3.5	Zulip Server before 2.1.3 allows XSS via a Markdown link, with resultant account takeover. **CVE ID : CVE-2020-10935**	https://blog.zulip.org/2020/04/01/zulip-server-2-1-3-security-release/	A-ZUL-ZULI-010520/184
Improper Restriction of Rendered UI Layers or Frames	20-04-2020	5.8	Zulip Server before 2.1.3 allows reverse tabnabbing via the Markdown functionality. **CVE ID : CVE-2020-9444**	https://blog.zulip.org/2020/04/01/zulip-server-2-1-3-security-release/	A-ZUL-ZULI-010520/185
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	20-04-2020	4.3	Zulip Server before 2.1.3 allows XSS via the modal_link feature in the Markdown functionality. **CVE ID : CVE-2020-9445**	https://blog.zulip.org/2020/04/01/zulip-server-2-1-3-security-release/	A-ZUL-ZULI-010520/186
Operating System					
Debian					
debian_linux					
Improper Neutralization of Input During Web Page	24-04-2020	4.3	GNU Mailman 2.x before 2.1.30 uses the .obj extension for scrubbed application/octet-stream	N/A	O-DEB-DEBI-010520/187

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Generation ('Cross-site Scripting')			MIME parts. This behavior may contribute to XSS attacks against list-archive visitors, because an HTTP reply from an archive web server may lack a MIME type, and a web browser may perform MIME sniffing, conclude that the MIME type should have been text/html, and execute JavaScript code. **CVE ID : CVE-2020-12137**		
Dlink					
dsl-2640b_firmware					
Insufficiently Protected Credentials	20-04-2020	5	An issue was discovered on D-Link DSL-2640B B2 EU_4.01B devices. A cfm UDP service listening on port 65002 allows remote, unauthenticated exfiltration of administrative credentials. **CVE ID : CVE-2020-9275**	N/A	O-DLI-DSL--010520/188
Out-of-bounds Write	20-04-2020	9	An issue was discovered on D-Link DSL-2640B B2 EU_4.01B devices. The function do_cgi(), which processes cgi requests supplied to the device's web servers, is vulnerable to a remotely exploitable stack-based buffer overflow. Unauthenticated exploitation is possible by	N/A	O-DLI-DSL--010520/189

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			combining this vulnerability with CVE-2020-9277. **CVE ID : CVE-2020-9276**		
Improper Authentication	20-04-2020	7.5	An issue was discovered on D-Link DSL-2640B B2 EU_4.01B devices. Authentication can be bypassed when accessing cgi modules. This allows one to perform administrative tasks (e.g., modify the admin password) with no authentication. **CVE ID : CVE-2020-9277**	N/A	O-DLI-DSL--010520/190
Improper Input Validation	20-04-2020	6.4	An issue was discovered on D-Link DSL-2640B B2 EU_4.01B devices. The device can be reset to its default configuration by accessing an unauthenticated URL. **CVE ID : CVE-2020-9278**	N/A	O-DLI-DSL--010520/191
Use of Hard-coded Credentials	20-04-2020	10	An issue was discovered on D-Link DSL-2640B B2 EU_4.01B devices. A hard-coded account allows management-interface login with high privileges. The logged-in user can perform critical tasks and take full control of the device. **CVE ID : CVE-2020-9279**	N/A	O-DLI-DSL--010520/192
evenroute					
iqrouter_firmware					
Improper	21-04-2020	7.5	IQrouter through 3.3.1,	N/A	O-EVE-IQRO-

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Neutralization of Special Elements used in an OS Command ('OS Command Injection')			when unconfigured, has multiple remote code execution vulnerabilities in the web-panel because of Bash Shell Metacharacter Injection. **CVE ID : CVE-2020-11963**		010520/193
Insufficiently Protected Credentials	21-04-2020	5	In IQrouter through 3.3.1, the Lua function diag_set_password in the web-panel allows remote attackers to change the root password arbitrarily. **CVE ID : CVE-2020-11964**	N/A	O-EVE-IQRO-010520/194
Insufficiently Protected Credentials	21-04-2020	7.5	In IQrouter through 3.3.1, there is a root user without a password, which allows attackers to gain full remote access via SSH. **CVE ID : CVE-2020-11965**	N/A	O-EVE-IQRO-010520/195
Weak Password Requirements	21-04-2020	7.5	In IQrouter through 3.3.1, the Lua function reset_password in the web-panel allows remote attackers to change the root password arbitrarily. **CVE ID : CVE-2020-11966**	N/A	O-EVE-IQRO-010520/196
Improper Privilege Management	21-04-2020	9	In IQrouter through 3.3.1, remote attackers can control the device (restart network, reboot, upgrade, reset) because of Incorrect Access Control.	N/A	O-EVE-IQRO-010520/197

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2020-11967		
Information Exposure Through Log Files	21-04-2020	5	In the web-panel in IQrouter through 3.3.1, remote attackers can read system logs because of Incorrect Access Control. **CVE ID : CVE-2020-11968**	N/A	O-EVE-IQRO-010520/198
Google					
android					
Out-of-bounds Read	17-04-2020	2.1	In f2fs_xattr_generic_list of xattr.c, there is a possible out of bounds read due to a missing bounds check. This could lead to local information disclosure with System execution privileges needed. User interaction is not required for exploitation.Product: Android. Versions: Android kernel. Android ID: A-120551147. **CVE ID : CVE-2020-0067**	https://source.android.com/security/bulletin/pixel/2020-04-01	O-GOO-ANDR-010520/199
Out-of-bounds Read	17-04-2020	2.1	In crus_afe_get_param of msm-cirrus-playback.c, there is a possible out of bounds read due to an integer overflow. This could lead to local information disclosure with System execution privileges needed. User interaction is not needed for exploitation.Product: Android. Versions: Android kernel. Android	https://source.android.com/security/bulletin/pixel/2020-04-01	O-GOO-ANDR-010520/200

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			ID: A-139354541 **CVE ID : CVE-2020-0068**		
Out-of-bounds Write	17-04-2020	10	In rw_t2t_update_lock_attributes of rw_t2t_ndef.cc, there is a possible out of bounds write due to a missing bounds check. This could lead to remote code execution over NFC with no additional execution privileges needed. User interaction is not needed for exploitation.Product: AndroidVersions: Android-8.0 Android-8.1 Android-9 Android-10Android ID: A-148159613 **CVE ID : CVE-2020-0070**	N/A	O-GOO-ANDR-010520/201
Out-of-bounds Write	17-04-2020	10	In rw_t2t_extract_default_locks_info of rw_t2t_ndef.cc, there is a possible out of bounds write due to a missing bounds check. This could lead to remote code execution over NFC with no additional execution privileges needed. User interaction is not needed for exploitation.Product: AndroidVersions: Android-8.0 Android-8.1 Android-9 Android-10Android ID: A-147310721	N/A	O-GOO-ANDR-010520/202

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2020-0071		
Out-of-bounds Write	17-04-2020	10	In rw_t2t_handle_tlv_detect_rsp of rw_t2t_ndef.cc, there is a possible out of bounds write due to a missing bounds check. This could lead to remote code execution over NFC with no additional execution privileges needed. User interaction is not needed for exploitation.Product: AndroidVersions: Android-8.0 Android-8.1 Android-9 Android-10Android ID: A-147310271 **CVE ID : CVE-2020-0072**	N/A	O-GOO-ANDR-010520/203
Out-of-bounds Write	17-04-2020	10	In rw_t2t_handle_tlv_detect_rsp of rw_t2t_ndef.cc, there is a possible out of bounds write due to a missing bounds check. This could lead to remote code execution over NFC with no additional execution privileges needed. User interaction is not needed for exploitation.Product: AndroidVersions: Android-8.0 Android-8.1 Android-9 Android-10Android ID: A-147309942 **CVE ID : CVE-2020-0073**	N/A	O-GOO-ANDR-010520/204

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Out-of-bounds Read	17-04-2020	2.1	In set_shared_key of the FPC IRIS TrustZone app, there is a possible out of bounds read due to a missing bounds check. This could lead to local information disclosure with System execution privileges needed. User interaction is not needed for exploitation.Product: AndroidVersions: Android kernelAndroid ID: A-146057864 **CVE ID : CVE-2020-0075**	N/A	O-GOO-ANDR-010520/205
Out-of-bounds Write	17-04-2020	4.6	In get_auth_result of the FPC IRIS TrustZone app, there is a possible out of bounds write due to a missing bounds check. This could lead to local escalation of privilege with System execution privileges needed. User interaction is not needed for exploitation.Product: AndroidVersions: Android kernelAndroid ID: A-146056878 **CVE ID : CVE-2020-0076**	N/A	O-GOO-ANDR-010520/206
Out-of-bounds Read	17-04-2020	2.1	In authorize_enroll of the FPC IRIS TrustZone app, there is a possible out of bounds read due to a missing bounds check. This could lead to local information disclosure with System execution privileges needed. User interaction is not needed	N/A	O-GOO-ANDR-010520/207

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			for exploitation.Product: AndroidVersions: Android kernelAndroid ID: A-146055840 **CVE ID : CVE-2020-0077**		
Out-of-bounds Write	17-04-2020	4.6	In releaseSecureStops of DrmPlugin.cpp, there is a possible out of bounds write due to a missing bounds check. This could lead to local escalation of privilege with no additional execution privileges needed. User interaction is not needed for exploitation.Product: AndroidVersions: Android-9 Android-10Android ID: A-144766455 **CVE ID : CVE-2020-0078**	N/A	O-GOO-ANDR-010520/208
Out-of-bounds Write	17-04-2020	4.6	In decrypt_1_2 of CryptoPlugin.cpp, there is a possible out of bounds write due to stale pointer. This could lead to local escalation of privilege with no additional execution privileges needed. User interaction is not needed for exploitation.Product: AndroidVersions: Android-9 Android-10Android ID: A-144506242 **CVE ID : CVE-2020-0079**	N/A	O-GOO-ANDR-010520/209
Improper Privilege	17-04-2020	9.3	In onOpActiveChanged and related methods of	N/A	O-GOO-ANDR-

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Management			AppOpsControllerImpl.java, there is a possible way to display an app overlaying other apps without the notification icon that it's overlaying. This could lead to local escalation of privilege with User execution privileges needed. User interaction is needed for exploitation.Product: AndroidVersions: Android-10Android ID: A-144092031 **CVE ID : CVE-2020-0080**		010520/210
Double Free	17-04-2020	7.2	In finalize of AssetManager.java, there is possible memory corruption due to a double free. This could lead to local escalation of privilege with no additional execution privileges needed. User interaction is not needed for exploitation.Product: AndroidVersions: Android-8.0 Android-8.1 Android-9 Android-10Android ID: A-144028297 **CVE ID : CVE-2020-0081**	N/A	O-GOO-ANDR-010520/211
Deserialization of Untrusted Data	17-04-2020	7.2	In ExternalVibration of ExternalVibration.java, there is a possible activation of an arbitrary intent due to unsafe deserialization. This could lead to local escalation of	N/A	O-GOO-ANDR-010520/212

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			privilege to system_server with no additional execution privileges needed. User interaction is not needed for exploitation.Product: AndroidVersions: Android-10Android ID: A-140417434 **CVE ID : CVE-2020-0082**		
Out-of-bounds Write	17-04-2020	7.5	An issue was discovered on LG mobile devices with Android OS 7.2, 8.0, 8.1, 9, and 10 software. A stack-based buffer overflow in the logging tool could allow an attacker to gain privileges. The LG ID is LVE-SMP-200005 (April 2020). **CVE ID : CVE-2020-11873**	https://lgsecurity.lge.com/	O-GOO-ANDR-010520/213
N/A	17-04-2020	5	An issue was discovered on LG mobile devices with Android OS 8.0, 8.1, 9, and 10 software. Attackers can bypass Factory Reset Protection (FRP). The LG ID is LVE-SMP-200004 (March 2020). **CVE ID : CVE-2020-11874**	https://lgsecurity.lge.com/	O-GOO-ANDR-010520/214
Improper Handling of Exceptional Conditions	17-04-2020	7.2	An issue was discovered on LG mobile devices with Android OS 8.0, 8.1, 9.0, and 10.0 (MTK chipsets) software. The MTK kernel does not properly implement exception	https://lgsecurity.lge.com/	O-GOO-ANDR-010520/215

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			handling, allowing an attacker to gain privileges. The LG ID is LVE-SMP-200001 (February 2020). **CVE ID : CVE-2020-11875**		
Huawei					
honor_v20_firmware					
Information Exposure	20-04-2020	2.9	Huawei smartphones Honor V20 with versions earlier than 10.0.0.179(C636E3R4P3), versions earlier than 10.0.0.180(C185E3R3P3), versions earlier than 10.0.0.180(C432E10R3P4) have an information disclosure vulnerability. The device does not sufficiently validate the identity of smart wearable device in certain specific scenario, the attacker need to gain certain information in the victim's smartphone to launch the attack, successful exploit could cause information disclosure. **CVE ID : CVE-2020-1803**	http://www.huawei.com/en/psirt/security-advisories/huawei-sa-20200415-02-smartphone-en, https://www.huawei.com/en/psirt/security-advisories/huawei-sa-20200415-02-smartphone-en	O-HUA-HONO-010520/216
taurus-al00b_firmware					
Information Exposure	20-04-2020	4.3	Huawei smartphones Taurus-AL00B with versions earlier than 10.0.0.205(C00E201R7P2) have an improper authentication	http://www.huawei.com/en/psirt/security-advisories/huawei-sa-	O-HUA-TAUR-010520/217

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			vulnerability. The software insufficiently validate the user's identity when a user wants to do certain operation. An attacker can trick user into installing a malicious application to exploit this vulnerability. Successful exploit may cause some information disclosure. **CVE ID : CVE-2020-9070**	20200415-01-smartphone-en, https://www.huawei.com/en/psirt/security-advisories/huawei-sa-20200415-01-smartphone-en	
Microsoft					
windows_nt					
Information Exposure	16-04-2020	5	**VERSION NOT SUPPORTED WHEN ASSIGNED** A vulnerability could cause certain data to be visible on the network when the 'password' feature is enabled. This vulnerability was discovered in and remediated in versions v4.9.1 and v4.10.1 on May 30, 2013. The 'password' feature is an additional optional check performed by TS1131 that it is connected to a specific controller. This data is sent as clear text and is visible on the network. This feature is not present in TriStation 1131 versions v4.9.1 and v4.10.1 through current.	N/A	O-MIC-WIND-010520/218

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Therefore, the vulnerability is not present in these versions. **CVE ID : CVE-2020-7483**		
N/A	16-04-2020	4.3	**VERSION NOT SUPPORTED WHEN ASSIGNED** A vulnerability with the former 'password' feature could allow a denial of service attack if the user is not following documented guidelines pertaining to dedicated TriStation connection and key-switch protection. This vulnerability was discovered and remediated in versions v4.9.1 and v4.10.1 on May 30, 2013. This feature is not present in version v4.9.1 and v4.10.1 through current. Therefore, the vulnerability is not present in these versions. **CVE ID : CVE-2020-7484**	N/A	O-MIC-WIND-010520/219
N/A	16-04-2020	7.5	**VERSION NOT SUPPORTED WHEN ASSIGNED** A legacy support account in the TriStation software version v4.9.0 and earlier could cause improper access to the TriStation host machine. This was addressed in TriStation version v4.9.1 and v4.10.1 released on May 30,	N/A	O-MIC-WIND-010520/220

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			2013.1 **CVE ID : CVE-2020-7485**		
windows					
Access of Resource Using Incompatible Type ('Type Confusion')	22-04-2020	6.8	This vulnerability allows remote attackers to execute arbitrary code on affected installations of Foxit PhantomPDF 9.7.0.29478. User interaction is required to exploit this vulnerability in that the target must visit a malicious page or open a malicious file. The specific flaw exists within the handling of the DuplicatePages command of the communication API. The issue results from the lack of proper validation of user-supplied data, which can result in a type confusion condition. An attacker can leverage this vulnerability to execute code in the context of the current process. Was ZDI-CAN-9828. **CVE ID : CVE-2020-10889**	N/A	O-MIC-WIND-010520/221
Cross-Site Request Forgery (CSRF)	22-04-2020	6.8	This vulnerability allows remote attackers to execute arbitrary code on affected installations of Foxit PhantomPDF 9.7.0.29478. User interaction is required to exploit this vulnerability in that the target must visit a malicious page or	N/A	O-MIC-WIND-010520/222

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			open a malicious file. The specific flaw exists within the communication API. The issue lies in the handling of the ConvertToPDF command, which allows an arbitrary file write with attacker controlled data. An attacker can leverage this vulnerability to execute code in the context of the current process. Was ZDI-CAN-9829. **CVE ID : CVE-2020-10890**		
Access of Resource Using Incompatible Type ('Type Confusion')	22-04-2020	6.8	This vulnerability allows remote attackers to execute arbitrary code on affected installations of Foxit PhantomPDF 9.7.0.29478. User interaction is required to exploit this vulnerability in that the target must visit a malicious page or open a malicious file. The specific flaw exists within the handling of the Save command of the communication API. The issue results from the lack of proper validation of user-supplied data, which can result in a type confusion condition. An attacker can leverage this vulnerability to execute code in the context of the current process. Was ZDI-	N/A	O-MIC-WIND-010520/223

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			CAN-9831. **CVE ID : CVE-2020-10891**		
Cross-Site Request Forgery (CSRF)	22-04-2020	6.8	This vulnerability allows remote attackers to execute arbitrary code on affected installations of Foxit PhantomPDF 9.7.0.29478. User interaction is required to exploit this vulnerability in that the target must visit a malicious page or open a malicious file. The specific flaw exists within the communication API. The issue lies in the handling of the CombineFiles command, which allows an arbitrary file write with attacker controlled data. An attacker can leverage this vulnerability to execute code in the context of the current process. Was ZDI-CAN-9830. **CVE ID : CVE-2020-10892**	N/A	O-MIC-WIND-010520/224
Out-of-bounds Read	22-04-2020	6.8	This vulnerability allows remote attackers to execute arbitrary code on affected installations of Foxit PhantomPDF 9.7.1.29511. User interaction is required to exploit this vulnerability in that the target must visit a malicious page or open a malicious file. The	N/A	O-MIC-WIND-010520/225

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			specific flaw exists within the handling of U3D objects in PDF files. The issue results from the lack of proper validation of user-supplied data, which can result in a read past the end of an allocated structure. An attacker can leverage this vulnerability to execute code in the context of the current process. Was ZDI-CAN-10191. **CVE ID : CVE-2020-10895**		
Out-of-bounds Read	22-04-2020	6.8	This vulnerability allows remote attackers to execute arbitrary code on affected installations of Foxit PhantomPDF 9.7.1.29511. User interaction is required to exploit this vulnerability in that the target must visit a malicious page or open a malicious file. The specific flaw exists within the handling of U3D objects in PDF files. The issue results from the lack of proper validation of user-supplied data, which can result in a read past the end of an allocated structure. An attacker can leverage this vulnerability to execute code in the context of the current process. Was ZDI-CAN-	N/A	O-MIC-WIND-010520/226

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			10195. **CVE ID : CVE-2020-10898**		
Use After Free	22-04-2020	6.8	This vulnerability allows remote attackers to execute arbitrary code on affected installations of Foxit Reader 9.7.1.29511. User interaction is required to exploit this vulnerability in that the target must visit a malicious page or open a malicious file. The specific flaw exists within the processing of XFA templates. The issue results from the lack of validating the existence of an object prior to performing operations on the object. An attacker can leverage this vulnerability to execute code in the context of the current process. Was ZDI-CAN-10132. **CVE ID : CVE-2020-10899**	N/A	O-MIC-WIND-010520/227
Use After Free	22-04-2020	6.8	This vulnerability allows remote attackers to execute arbitrary code on affected installations of Foxit Reader 9.7.1.29511. User interaction is required to exploit this vulnerability in that the target must visit a malicious page or open a malicious file. The specific	N/A	O-MIC-WIND-010520/228

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			flaw exists within the processing of AcroForms. The issue results from the lack of validating the existence of an object prior to performing operations on the object. An attacker can leverage this vulnerability to execute code in the context of the current process. Was ZDI-CAN-10142. **CVE ID : CVE-2020-10900**		
Out-of-bounds Read	22-04-2020	4.3	This vulnerability allows remote attackers to disclose sensitive information on affected installations of Foxit PhantomPDF 9.7.1.29511. User interaction is required to exploit this vulnerability in that the target must visit a malicious page or open a malicious file. The specific flaw exists within the handling of U3D objects embedded in a PDF. The issue results from the lack of proper validation of user-supplied data, which can result in a read past the end of an allocated object. An attacker can leverage this in conjunction with other vulnerabilities to execute code in the context of the current process. Was ZDI-	N/A	O-MIC-WIND-010520/229

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			CAN-10463. **CVE ID : CVE-2020-10903**		
Improper Input Validation	22-04-2020	7.2	Improper Input Validation in Plex Media Server on Windows allows a local, unauthenticated attacker to execute arbitrary Python code with SYSTEM privileges. **CVE ID : CVE-2020-5740**	https://www.tenable.com/security/research/tra-2020-25	O-MIC-WIND-010520/230
windows_xp					
Information Exposure	16-04-2020	5	**VERSION NOT SUPPORTED WHEN ASSIGNED** A vulnerability could cause certain data to be visible on the network when the 'password' feature is enabled. This vulnerability was discovered in and remediated in versions v4.9.1 and v4.10.1 on May 30, 2013. The 'password' feature is an additional optional check performed by TS1131 that it is connected to a specific controller. This data is sent as clear text and is visible on the network. This feature is not present in TriStation 1131 versions v4.9.1 and v4.10.1 through current. Therefore, the vulnerability is not	N/A	O-MIC-WIND-010520/231

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			present in these versions. **CVE ID : CVE-2020-7483**		
N/A	16-04-2020	4.3	**VERSION NOT SUPPORTED WHEN ASSIGNED** A vulnerability with the former 'password' feature could allow a denial of service attack if the user is not following documented guidelines pertaining to dedicated TriStation connection and key-switch protection. This vulnerability was discovered and remediated in versions v4.9.1 and v4.10.1 on May 30, 2013. This feature is not present in version v4.9.1 and v4.10.1 through current. Therefore, the vulnerability is not present in these versions. **CVE ID : CVE-2020-7484**	N/A	O-MIC-WIND-010520/232
N/A	16-04-2020	7.5	**VERSION NOT SUPPORTED WHEN ASSIGNED** A legacy support account in the TriStation software version v4.9.0 and earlier could cause improper access to the TriStation host machine. This was addressed in TriStation version v4.9.1 and v4.10.1 released on May 30, 2013.1	N/A	O-MIC-WIND-010520/233

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2020-7485		
windows_7					
Information Exposure	16-04-2020	5	**VERSION NOT SUPPORTED WHEN ASSIGNED** A vulnerability could cause certain data to be visible on the network when the 'password' feature is enabled. This vulnerability was discovered in and remediated in versions v4.9.1 and v4.10.1 on May 30, 2013. The 'password' feature is an additional optional check performed by TS1131 that it is connected to a specific controller. This data is sent as clear text and is visible on the network. This feature is not present in TriStation 1131 versions v4.9.1 and v4.10.1 through current. Therefore, the vulnerability is not present in these versions. **CVE ID : CVE-2020-7483**	N/A	O-MIC-WIND-010520/234
N/A	16-04-2020	4.3	**VERSION NOT SUPPORTED WHEN ASSIGNED** A vulnerability with the former 'password' feature could allow a denial of service attack if the user is not following documented guidelines pertaining to dedicated	N/A	O-MIC-WIND-010520/235

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			TriStation connection and key-switch protection. This vulnerability was discovered and remediated in versions v4.9.1 and v4.10.1 on May 30, 2013. This feature is not present in version v4.9.1 and v4.10.1 through current. Therefore, the vulnerability is not present in these versions. **CVE ID : CVE-2020-7484**		
N/A	16-04-2020	7.5	**VERSION NOT SUPPORTED WHEN ASSIGNED** A legacy support account in the TriStation software version v4.9.0 and earlier could cause improper access to the TriStation host machine. This was addressed in TriStation version v4.9.1 and v4.10.1 released on May 30, 2013.1 **CVE ID : CVE-2020-7485**	N/A	O-MIC-WIND-010520/236
Netapp					
clustered_data_ontap					
Uncontrolled Resource Consumption	17-04-2020	5	ntpd in ntp before 4.2.8p14 and 4.3.x before 4.3.100 allows an off-path attacker to block unauthenticated synchronization via a server mode packet with a spoofed source IP address, because	https://security.netapp.com/advisory/ntap-20200424-0002/	O-NET-CLUS-010520/237

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			transmissions are rescheduled even when a packet lacks a valid origin timestamp. **CVE ID : CVE-2020-11868**		
oppo					
coloros					
Information Exposure	21-04-2020	5	In ColorOS (oppo mobile phone operating system, based on AOSP frameworks/native code position/services/surface flinger surfaceflinger.CPP), RGB is defined on the stack but uninitialized, so when the screenShot function to RGB value assignment, will not initialize the value is returned to the attackers, leading to values on the stack information leakage, the vulnerability can be used to bypass attackers ALSR. **CVE ID : CVE-2020-11828**	https://security.oppo.com/cn/noticedetails.html?noticeId=2020158734830 0033	O-OPP-COLO-010520/238
Qualcomm					
qca6574au_firmware					
Reachable Assertion	16-04-2020	7.8	Active command timeout since WM status change cmd is not removed from active queue if peer sends multiple deauth frames. in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer Electronics Connectivity,	https://www.qualcomm.com/company/product-security/bulletins/april-2020-bulletin	O-QUA-QCA6-010520/239

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables in APQ8009, APQ8017, APQ8053, APQ8096AU, MDM9206, MDM9207C, MDM9607, MDM9640, MDM9650, MSM8905, MSM8909W, MSM8917, MSM8920, MSM8937, MSM8940, MSM8953, MSM8996AU, QCA6174A, QCA6574AU, QCA9377, QCA9379, QCM2150, QCN7605, QCS605, QM215, SC8180X, SDM429, SDM429W, SDM439, SDM450, SDM630, SDM632, SDM636, SDM660, SDM845, SDX20, SDX24, SDX55, SM8150, SXR1130 **CVE ID : CVE-2020-3651**		
qca6174a_firmware					
Reachable Assertion	16-04-2020	7.8	Active command timeout since WM status change cmd is not removed from active queue if peer sends multiple deauth frames. in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT,	https://www.qualcomm.com/company/product-security/bulletins/april-2020-bulletin	O-QUA-QCA6-010520/240

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables in APQ8009, APQ8017, APQ8053, APQ8096AU, MDM9206, MDM9207C, MDM9607, MDM9640, MDM9650, MSM8905, MSM8909W, MSM8917, MSM8920, MSM8937, MSM8940, MSM8953, MSM8996AU, QCA6174A, QCA6574AU, QCA9377, QCA9379, QCM2150, QCN7605, QCS605, QM215, SC8180X, SDM429, SDM429W, SDM439, SDM450, SDM630, SDM632, SDM636, SDM660, SDM845, SDX20, SDX24, SDX55, SM8150, SXR1130 **CVE ID : CVE-2020-3651**		
qca9377_firmware					
Reachable Assertion	16-04-2020	7.8	Active command timeout since WM status change cmd is not removed from active queue if peer sends multiple deauth frames. in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon	https://www.qualcomm.com/company/product-security/bulletins/april-2020-bulletin	O-QUA-QCA9-010520/241

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Wearables in APQ8009, APQ8017, APQ8053, APQ8096AU, MDM9206, MDM9207C, MDM9607, MDM9640, MDM9650, MSM8905, MSM8909W, MSM8917, MSM8920, MSM8937, MSM8940, MSM8953, MSM8996AU, QCA6174A, QCA6574AU, QCA9377, QCA9379, QCM2150, QCN7605, QCS605, QM215, SC8180X, SDM429, SDM429W, SDM439, SDM450, SDM630, SDM632, SDM636, SDM660, SDM845, SDX20, SDX24, SDX55, SM8150, SXR1130 **CVE ID : CVE-2020-3651**		
qca9379_firmware					
Reachable Assertion	16-04-2020	7.8	Active command timeout since WM status change cmd is not removed from active queue if peer sends multiple deauth frames. in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables in APQ8009, APQ8017, APQ8053, APQ8096AU, MDM9206,	https://www.qualcomm.com/company/product-security/bulletins/april-2020-bulletin	O-QUA-QCA9-010520/242

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			MDM9207C, MDM9607, MDM9640, MDM9650, MSM8905, MSM8909W, MSM8917, MSM8920, MSM8937, MSM8940, MSM8953, MSM8996AU, QCA6174A, QCA6574AU, QCA9377, QCA9379, QCM2150, QCN7605, QCS605, QM215, SC8180X, SDM429, SDM429W, SDM439, SDM450, SDM630, SDM632, SDM636, SDM660, SDM845, SDX20, SDX24, SDX55, SM8150, SXR1130 **CVE ID : CVE-2020-3651**		
sdm429w_firmware					
Reachable Assertion	16-04-2020	7.8	Active command timeout since WM status change cmd is not removed from active queue if peer sends multiple deauth frames. in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables in APQ8009, APQ8017, APQ8053, APQ8096AU, MDM9206, MDM9207C, MDM9607, MDM9640, MDM9650, MSM8905, MSM8909W,	https://www.qualcomm.com/company/product-security/bulletins/april-2020-bulletin	O-QUA-SDM4-010520/243

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			MSM8917, MSM8920, MSM8937, MSM8940, MSM8953, MSM8996AU, QCA6174A, QCA6574AU, QCA9377, QCA9379, QCM2150, QCN7605, QCS605, QM215, SC8180X, SDM429, SDM429W, SDM439, SDM450, SDM630, SDM632, SDM636, SDM660, SDM845, SDX20, SDX24, SDX55, SM8150, SXR1130 **CVE ID : CVE-2020-3651**		
sc7180_firmware					
Out-of-bounds Read	16-04-2020	9.4	Possible buffer over-read issue in windows x86 wlan driver function while processing beacon or request frame due to lack of check of length of variable received. in Snapdragon Compute, Snapdragon Connectivity in MSM8998, QCA6390, SC7180, SC8180X, SDM850 **CVE ID : CVE-2020-3652**	https://www.qualcomm.com/company/product-security/bulletins/april-2020-bulletin	O-QUA-SC71-010520/244
Out-of-bounds Read	16-04-2020	9.4	Possible buffer over-read in windows wlan driver function due to lack of check of length of variable received from userspace in Snapdragon Compute, Snapdragon Connectivity in MSM8998, QCA6390, SC7180, SC8180X, SDM850	https://www.qualcomm.com/company/product-security/bulletins/april-2020-bulletin	O-QUA-SC71-010520/245

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2020-3653		
apq8009_firmware					
Reachable Assertion	16-04-2020	7.8	Active command timeout since WM status change cmd is not removed from active queue if peer sends multiple deauth frames. in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables in APQ8009, APQ8017, APQ8053, APQ8096AU, MDM9206, MDM9207C, MDM9607, MDM9640, MDM9650, MSM8905, MSM8909W, MSM8917, MSM8920, MSM8937, MSM8940, MSM8953, MSM8996AU, QCA6174A, QCA6574AU, QCA9377, QCA9379, QCM2150, QCN7605, QCS605, QM215, SC8180X, SDM429, SDM429W, SDM439, SDM450, SDM630, SDM632, SDM636, SDM660, SDM845, SDX20, SDX24, SDX55, SM8150, SXR1130 **CVE ID : CVE-2020-3651**	https://www.qualcomm.com/company/product-security/bulletins/april-2020-bulletin	O-QUA-APQ8-010520/246
msm8953_firmware					

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Reachable Assertion	16-04-2020	7.8	Active command timeout since WM status change cmd is not removed from active queue if peer sends multiple deauth frames. in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables in APQ8009, APQ8017, APQ8053, APQ8096AU, MDM9206, MDM9207C, MDM9607, MDM9640, MDM9650, MSM8905, MSM8909W, MSM8917, MSM8920, MSM8937, MSM8940, MSM8953, MSM8996AU, QCA6174A, QCA6574AU, QCA9377, QCA9379, QCM2150, QCN7605, QCS605, QM215, SC8180X, SDM429, SDM429W, SDM439, SDM450, SDM630, SDM632, SDM636, SDM660, SDM845, SDX20, SDX24, SDX55, SM8150, SXR1130 **CVE ID : CVE-2020-3651**	https://www.qualcomm.com/company/product-security/bulletins/april-2020-bulletin	O-QUA-MSM8-010520/247
msm8998_firmware					
Out-of-bounds Read	16-04-2020	9.4	Possible buffer over-read issue in windows x86 wlan driver function	https://www.qualcomm.com/compan	O-QUA-MSM8-010520/248

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			while processing beacon or request frame due to lack of check of length of variable received. in Snapdragon Compute, Snapdragon Connectivity in MSM8998, QCA6390, SC7180, SC8180X, SDM850 **CVE ID : CVE-2020-3652**	y/product-security/bulletins/april-2020-bulletin	
Out-of-bounds Read	16-04-2020	9.4	Possible buffer over-read in windows wlan driver function due to lack of check of length of variable received from userspace in Snapdragon Compute, Snapdragon Connectivity in MSM8998, QCA6390, SC7180, SC8180X, SDM850 **CVE ID : CVE-2020-3653**	https://www.qualcomm.com/company/product-security/bulletins/april-2020-bulletin	O-QUA-MSM8-010520/249
apq8053_firmware					
Reachable Assertion	16-04-2020	7.8	Active command timeout since WM status change cmd is not removed from active queue if peer sends multiple deauth frames. in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables in APQ8009, APQ8017, APQ8053, APQ8096AU, MDM9206,	https://www.qualcomm.com/company/product-security/bulletins/april-2020-bulletin	O-QUA-APQ8-010520/250

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			MDM9207C, MDM9607, MDM9640, MDM9650, MSM8905, MSM8909W, MSM8917, MSM8920, MSM8937, MSM8940, MSM8953, MSM8996AU, QCA6174A, QCA6574AU, QCA9377, QCA9379, QCM2150, QCN7605, QCS605, QM215, SC8180X, SDM429, SDM429W, SDM439, SDM450, SDM630, SDM632, SDM636, SDM660, SDM845, SDX20, SDX24, SDX55, SM8150, SXR1130 **CVE ID : CVE-2020-3651**		
mdm9207c_firmware					
Reachable Assertion	16-04-2020	7.8	Active command timeout since WM status change cmd is not removed from active queue if peer sends multiple deauth frames. in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables in APQ8009, APQ8017, APQ8053, APQ8096AU, MDM9206, MDM9207C, MDM9607, MDM9640, MDM9650, MSM8905, MSM8909W,	https://www.qualcomm.com/company/product-security/bulletins/april-2020-bulletin	O-QUA-MDM9-010520/251

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			MSM8917, MSM8920, MSM8937, MSM8940, MSM8953, MSM8996AU, QCA6174A, QCA6574AU, QCA9377, QCA9379, QCM2150, QCN7605, QCS605, QM215, SC8180X, SDM429, SDM429W, SDM439, SDM450, SDM630, SDM632, SDM636, SDM660, SDM845, SDX20, SDX24, SDX55, SM8150, SXR1130 **CVE ID : CVE-2020-3651**		
msm8905_firmware					
Reachable Assertion	16-04-2020	7.8	Active command timeout since WM status change cmd is not removed from active queue if peer sends multiple deauth frames. in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables in APQ8009, APQ8017, APQ8053, APQ8096AU, MDM9206, MDM9207C, MDM9607, MDM9640, MDM9650, MSM8905, MSM8909W, MSM8917, MSM8920, MSM8937, MSM8940, MSM8953, MSM8996AU,	https://www.qualcomm.com/company/product-security/bulletins/april-2020-bulletin	O-QUA-MSM8-010520/252

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			QCA6174A, QCA6574AU, QCA9377, QCA9379, QCM2150, QCN7605, QCS605, QM215, SC8180X, SDM429, SDM429W, SDM439, SDM450, SDM630, SDM632, SDM636, SDM660, SDM845, SDX20, SDX24, SDX55, SM8150, SXR1130 **CVE ID : CVE-2020-3651**		
qcn7605_firmware					
Reachable Assertion	16-04-2020	7.8	Active command timeout since WM status change cmd is not removed from active queue if peer sends multiple deauth frames. in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables in APQ8009, APQ8017, APQ8053, APQ8096AU, MDM9206, MDM9207C, MDM9607, MDM9640, MDM9650, MSM8905, MSM8909W, MSM8917, MSM8920, MSM8937, MSM8940, MSM8953, MSM8996AU, QCA6174A, QCA6574AU, QCA9377, QCA9379, QCM2150, QCN7605,	https://www.qualcomm.com/company/product-security/bulletins/april-2020-bulletin	O-QUA-QCN7-010520/253

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			QCS605, QM215, SC8180X, SDM429, SDM429W, SDM439, SDM450, SDM630, SDM632, SDM636, SDM660, SDM845, SDX20, SDX24, SDX55, SM8150, SXR1130 **CVE ID : CVE-2020-3651**		
sdm845_firmware					
Reachable Assertion	16-04-2020	7.8	Active command timeout since WM status change cmd is not removed from active queue if peer sends multiple deauth frames. in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables in APQ8009, APQ8017, APQ8053, APQ8096AU, MDM9206, MDM9207C, MDM9607, MDM9640, MDM9650, MSM8905, MSM8909W, MSM8917, MSM8920, MSM8937, MSM8940, MSM8953, MSM8996AU, QCA6174A, QCA6574AU, QCA9377, QCA9379, QCM2150, QCN7605, QCS605, QM215, SC8180X, SDM429, SDM429W, SDM439,	https://www.qualcomm.com/company/product-security/bulletins/april-2020-bulletin	O-QUA-SDM8-010520/254

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			SDM450, SDM630, SDM632, SDM636, SDM660, SDM845, SDX20, SDX24, SDX55, SM8150, SXR1130 **CVE ID : CVE-2020-3651**		
apq8017_firmware					
Reachable Assertion	16-04-2020	7.8	Active command timeout since WM status change cmd is not removed from active queue if peer sends multiple deauth frames. in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables in APQ8009, APQ8017, APQ8053, APQ8096AU, MDM9206, MDM9207C, MDM9607, MDM9640, MDM9650, MSM8905, MSM8909W, MSM8917, MSM8920, MSM8937, MSM8940, MSM8953, MSM8996AU, QCA6174A, QCA6574AU, QCA9377, QCA9379, QCM2150, QCN7605, QCS605, QM215, SC8180X, SDM429, SDM429W, SDM439, SDM450, SDM630, SDM632, SDM636, SDM660, SDM845, SDX20,	https://www.qualcomm.com/company/product-security/bulletins/april-2020-bulletin	O-QUA-APQ8-010520/255

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			SDX24, SDX55, SM8150, SXR1130 **CVE ID : CVE-2020-3651**		
apq8096au_firmware					
Reachable Assertion	16-04-2020	7.8	Active command timeout since WM status change cmd is not removed from active queue if peer sends multiple deauth frames. in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables in APQ8009, APQ8017, APQ8053, APQ8096AU, MDM9206, MDM9207C, MDM9607, MDM9640, MDM9650, MSM8905, MSM8909W, MSM8917, MSM8920, MSM8937, MSM8940, MSM8953, MSM8996AU, QCA6174A, QCA6574AU, QCA9377, QCA9379, QCM2150, QCN7605, QCS605, QM215, SC8180X, SDM429, SDM429W, SDM439, SDM450, SDM630, SDM632, SDM636, SDM660, SDM845, SDX20, SDX24, SDX55, SM8150, SXR1130 **CVE ID : CVE-2020-3651**	https://www.qualcomm.com/company/product-security/bulletins/april-2020-bulletin	O-QUA-APQ8-010520/256

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
sdm636_firmware					
Reachable Assertion	16-04-2020	7.8	Active command timeout since WM status change cmd is not removed from active queue if peer sends multiple deauth frames. in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables in APQ8009, APQ8017, APQ8053, APQ8096AU, MDM9206, MDM9207C, MDM9607, MDM9640, MDM9650, MSM8905, MSM8909W, MSM8917, MSM8920, MSM8937, MSM8940, MSM8953, MSM8996AU, QCA6174A, QCA6574AU, QCA9377, QCA9379, QCM2150, QCN7605, QCS605, QM215, SC8180X, SDM429, SDM429W, SDM439, SDM450, SDM630, SDM632, SDM636, SDM660, SDM845, SDX20, SDX24, SDX55, SM8150, SXR1130 **CVE ID : CVE-2020-3651**	https://www.qualcomm.com/company/product-security/bulletins/april-2020-bulletin	O-QUA-SDM6-010520/257
qm215_firmware					
Reachable Assertion	16-04-2020	7.8	Active command timeout since WM status change	https://www.qualcomm.	O-QUA-QM21-

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			cmd is not removed from active queue if peer sends multiple deauth frames. in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables in APQ8009, APQ8017, APQ8053, APQ8096AU, MDM9206, MDM9207C, MDM9607, MDM9640, MDM9650, MSM8905, MSM8909W, MSM8917, MSM8920, MSM8937, MSM8940, MSM8953, MSM8996AU, QCA6174A, QCA6574AU, QCA9377, QCA9379, QCM2150, QCN7605, QCS605, QM215, SC8180X, SDM429, SDM429W, SDM439, SDM450, SDM630, SDM632, SDM636, SDM660, SDM845, SDX20, SDX24, SDX55, SM8150, SXR1130 **CVE ID : CVE-2020-3651**	com/company/product-security/bulletins/april-2020-bulletin	010520/258
sm8150_firmware					
Reachable Assertion	16-04-2020	7.8	Active command timeout since WM status change cmd is not removed from active queue if peer sends multiple deauth frames. in	https://www.qualcomm.com/company/product-security/bull	O-QUA-SM81-010520/259

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables in APQ8009, APQ8017, APQ8053, APQ8096AU, MDM9206, MDM9207C, MDM9607, MDM9640, MDM9650, MSM8905, MSM8909W, MSM8917, MSM8920, MSM8937, MSM8940, MSM8953, MSM8996AU, QCA6174A, QCA6574AU, QCA9377, QCA9379, QCM2150, QCN7605, QCS605, QM215, SC8180X, SDM429, SDM429W, SDM439, SDM450, SDM630, SDM632, SDM636, SDM660, SDM845, SDX20, SDX24, SDX55, SM8150, SXR1130 **CVE ID : CVE-2020-3651**	etins/april-2020-bulletin	
mdm9206_firmware					
Reachable Assertion	16-04-2020	7.8	Active command timeout since WM status change cmd is not removed from active queue if peer sends multiple deauth frames. in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer	https://www.qualcomm.com/company/product-security/bulletins/april-2020-bulletin	O-QUA-MDM9-010520/260

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables in APQ8009, APQ8017, APQ8053, APQ8096AU, MDM9206, MDM9207C, MDM9607, MDM9640, MDM9650, MSM8905, MSM8909W, MSM8917, MSM8920, MSM8937, MSM8940, MSM8953, MSM8996AU, QCA6174A, QCA6574AU, QCA9377, QCA9379, QCM2150, QCN7605, QCS605, QM215, SC8180X, SDM429, SDM429W, SDM439, SDM450, SDM630, SDM632, SDM636, SDM660, SDM845, SDX20, SDX24, SDX55, SM8150, SXR1130 **CVE ID : CVE-2020-3651**		
mdm9607_firmware					
Reachable Assertion	16-04-2020	7.8	Active command timeout since WM status change cmd is not removed from active queue if peer sends multiple deauth frames. in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon	https://www.qualcomm.com/company/product-security/bulletins/april-2020-bulletin	O-QUA-MDM9-010520/261

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables in APQ8009, APQ8017, APQ8053, APQ8096AU, MDM9206, MDM9207C, MDM9607, MDM9640, MDM9650, MSM8905, MSM8909W, MSM8917, MSM8920, MSM8937, MSM8940, MSM8953, MSM8996AU, QCA6174A, QCA6574AU, QCA9377, QCA9379, QCM2150, QCN7605, QCS605, QM215, SC8180X, SDM429, SDM429W, SDM439, SDM450, SDM630, SDM632, SDM636, SDM660, SDM845, SDX20, SDX24, SDX55, SM8150, SXR1130 **CVE ID : CVE-2020-3651**		
mdm9650_firmware					
Reachable Assertion	16-04-2020	7.8	Active command timeout since WM status change cmd is not removed from active queue if peer sends multiple deauth frames. in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice &	https://www.qualcomm.com/company/product-security/bulletins/april-2020-bulletin	O-QUA-MDM9-010520/262

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Music, Snapdragon Wearables in APQ8009, APQ8017, APQ8053, APQ8096AU, MDM9206, MDM9207C, MDM9607, MDM9640, MDM9650, MSM8905, MSM8909W, MSM8917, MSM8920, MSM8937, MSM8940, MSM8953, MSM8996AU, QCA6174A, QCA6574AU, QCA9377, QCA9379, QCM2150, QCN7605, QCS605, QM215, SC8180X, SDM429, SDM429W, SDM439, SDM450, SDM630, SDM632, SDM636, SDM660, SDM845, SDX20, SDX24, SDX55, SM8150, SXR1130 **CVE ID : CVE-2020-3651**		
msm8996au_firmware					
Reachable Assertion	16-04-2020	7.8	Active command timeout since WM status change cmd is not removed from active queue if peer sends multiple deauth frames. in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables in APQ8009, APQ8017, APQ8053,	https://www.qualcomm.com/company/product-security/bulletins/april-2020-bulletin	O-QUA-MSM8-010520/263

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			APQ8096AU, MDM9206, MDM9207C, MDM9607, MDM9640, MDM9650, MSM8905, MSM8909W, MSM8917, MSM8920, MSM8937, MSM8940, MSM8953, MSM8996AU, QCA6174A, QCA6574AU, QCA9377, QCA9379, QCM2150, QCN7605, QCS605, QM215, SC8180X, SDM429, SDM429W, SDM439, SDM450, SDM630, SDM632, SDM636, SDM660, SDM845, SDX20, SDX24, SDX55, SM8150, SXR1130 **CVE ID : CVE-2020-3651**		
sdm429_firmware					
Reachable Assertion	16-04-2020	7.8	Active command timeout since WM status change cmd is not removed from active queue if peer sends multiple deauth frames. in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables in APQ8009, APQ8017, APQ8053, APQ8096AU, MDM9206, MDM9207C, MDM9607, MDM9640, MDM9650,	https://www.qualcomm.com/company/product-security/bulletins/april-2020-bulletin	O-QUA-SDM4-010520/264

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			MSM8905, MSM8909W, MSM8917, MSM8920, MSM8937, MSM8940, MSM8953, MSM8996AU, QCA6174A, QCA6574AU, QCA9377, QCA9379, QCM2150, QCN7605, QCS605, QM215, SC8180X, SDM429, SDM429W, SDM439, SDM450, SDM630, SDM632, SDM636, SDM660, SDM845, SDX20, SDX24, SDX55, SM8150, SXR1130 **CVE ID : CVE-2020-3651**		
sdm632_firmware					
Reachable Assertion	16-04-2020	7.8	Active command timeout since WM status change cmd is not removed from active queue if peer sends multiple deauth frames. in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables in APQ8009, APQ8017, APQ8053, APQ8096AU, MDM9206, MDM9207C, MDM9607, MDM9640, MDM9650, MSM8905, MSM8909W, MSM8917, MSM8920, MSM8937, MSM8940,	https://www.qualcomm.com/company/product-security/bulletins/april-2020-bulletin	O-QUA-SDM6-010520/265

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			MSM8953, MSM8996AU, QCA6174A, QCA6574AU, QCA9377, QCA9379, QCM2150, QCN7605, QCS605, QM215, SC8180X, SDM429, SDM429W, SDM439, SDM450, SDM630, SDM632, SDM636, SDM660, SDM845, SDX20, SDX24, SDX55, SM8150, SXR1130 **CVE ID : CVE-2020-3651**		
msm8917_firmware					
Reachable Assertion	16-04-2020	7.8	Active command timeout since WM status change cmd is not removed from active queue if peer sends multiple deauth frames. in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables in APQ8009, APQ8017, APQ8053, APQ8096AU, MDM9206, MDM9207C, MDM9607, MDM9640, MDM9650, MSM8905, MSM8909W, MSM8917, MSM8920, MSM8937, MSM8940, MSM8953, MSM8996AU, QCA6174A, QCA6574AU, QCA9377, QCA9379,	https://www.qualcomm.com/company/product-security/bulletins/april-2020-bulletin	O-QUA-MSM8-010520/266

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			QCM2150, QCN7605, QCS605, QM215, SC8180X, SDM429, SDM429W, SDM439, SDM450, SDM630, SDM632, SDM636, SDM660, SDM845, SDX20, SDX24, SDX55, SM8150, SXR1130 **CVE ID : CVE-2020-3651**		
msm8920_firmware					
Reachable Assertion	16-04-2020	7.8	Active command timeout since WM status change cmd is not removed from active queue if peer sends multiple deauth frames. in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables in APQ8009, APQ8017, APQ8053, APQ8096AU, MDM9206, MDM9207C, MDM9607, MDM9640, MDM9650, MSM8905, MSM8909W, MSM8917, MSM8920, MSM8937, MSM8940, MSM8953, MSM8996AU, QCA6174A, QCA6574AU, QCA9377, QCA9379, QCM2150, QCN7605, QCS605, QM215, SC8180X, SDM429,	https://www.qualcomm.com/company/product-security/bulletins/april-2020-bulletin	O-QUA-MSM8-010520/267

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			SDM429W, SDM439, SDM450, SDM630, SDM632, SDM636, SDM660, SDM845, SDX20, SDX24, SDX55, SM8150, SXR1130 **CVE ID : CVE-2020-3651**		
msm8937_firmware					
Reachable Assertion	16-04-2020	7.8	Active command timeout since WM status change cmd is not removed from active queue if peer sends multiple deauth frames. in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables in APQ8009, APQ8017, APQ8053, APQ8096AU, MDM9206, MDM9207C, MDM9607, MDM9640, MDM9650, MSM8905, MSM8909W, MSM8917, MSM8920, MSM8937, MSM8940, MSM8953, MSM8996AU, QCA6174A, QCA6574AU, QCA9377, QCA9379, QCM2150, QCN7605, QCS605, QM215, SC8180X, SDM429, SDM429W, SDM439, SDM450, SDM630, SDM632, SDM636,	https://www.qualcomm.com/company/product-security/bulletins/april-2020-bulletin	O-QUA-MSM8-010520/268

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			SDM660, SDM845, SDX20, SDX24, SDX55, SM8150, SXR1130 **CVE ID : CVE-2020-3651**		
msm8940_firmware					
Reachable Assertion	16-04-2020	7.8	Active command timeout since WM status change cmd is not removed from active queue if peer sends multiple deauth frames. in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables in APQ8009, APQ8017, APQ8053, APQ8096AU, MDM9206, MDM9207C, MDM9607, MDM9640, MDM9650, MSM8905, MSM8909W, MSM8917, MSM8920, MSM8937, MSM8940, MSM8953, MSM8996AU, QCA6174A, QCA6574AU, QCA9377, QCA9379, QCM2150, QCN7605, QCS605, QM215, SC8180X, SDM429, SDM429W, SDM439, SDM450, SDM630, SDM632, SDM636, SDM660, SDM845, SDX20, SDX24, SDX55, SM8150, SXR1130	https://www.qualcomm.com/company/product-security/bulletins/april-2020-bulletin	O-QUA-MSM8-010520/269

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2020-3651		
sdm450_firmware					
Reachable Assertion	16-04-2020	7.8	Active command timeout since WM status change cmd is not removed from active queue if peer sends multiple deauth frames. in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables in APQ8009, APQ8017, APQ8053, APQ8096AU, MDM9206, MDM9207C, MDM9607, MDM9640, MDM9650, MSM8905, MSM8909W, MSM8917, MSM8920, MSM8937, MSM8940, MSM8953, MSM8996AU, QCA6174A, QCA6574AU, QCA9377, QCA9379, QCM2150, QCN7605, QCS605, QM215, SC8180X, SDM429, SDM429W, SDM439, SDM450, SDM630, SDM632, SDM636, SDM660, SDM845, SDX20, SDX24, SDX55, SM8150, SXR1130 **CVE ID : CVE-2020-3651**	https://www.qualcomm.com/company/product-security/bulletins/april-2020-bulletin	O-QUA-SDM4-010520/270
sc8180x_firmware					

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Reachable Assertion	16-04-2020	7.8	Active command timeout since WM status change cmd is not removed from active queue if peer sends multiple deauth frames. in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables in APQ8009, APQ8017, APQ8053, APQ8096AU, MDM9206, MDM9207C, MDM9607, MDM9640, MDM9650, MSM8905, MSM8909W, MSM8917, MSM8920, MSM8937, MSM8940, MSM8953, MSM8996AU, QCA6174A, QCA6574AU, QCA9377, QCA9379, QCM2150, QCN7605, QCS605, QM215, SC8180X, SDM429, SDM429W, SDM439, SDM450, SDM630, SDM632, SDM636, SDM660, SDM845, SDX20, SDX24, SDX55, SM8150, SXR1130 **CVE ID : CVE-2020-3651**	https://www.qualcomm.com/company/product-security/bulletins/april-2020-bulletin	O-QUA-SC81-010520/271
Out-of-bounds Read	16-04-2020	9.4	Possible buffer over-read issue in windows x86 wlan driver function while processing beacon or request frame due to	https://www.qualcomm.com/company/product-security/bull	O-QUA-SC81-010520/272

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			lack of check of length of variable received. in Snapdragon Compute, Snapdragon Connectivity in MSM8998, QCA6390, SC7180, SC8180X, SDM850 **CVE ID : CVE-2020-3652**	etins/april-2020-bulletin	
Out-of-bounds Read	16-04-2020	9.4	Possible buffer over-read in windows wlan driver function due to lack of check of length of variable received from userspace in Snapdragon Compute, Snapdragon Connectivity in MSM8998, QCA6390, SC7180, SC8180X, SDM850 **CVE ID : CVE-2020-3653**	https://www.qualcomm.com/company/product-security/bulletins/april-2020-bulletin	O-QUA-SC81-010520/273
sdm850_firmware					
Out-of-bounds Read	16-04-2020	9.4	Possible buffer over-read issue in windows x86 wlan driver function while processing beacon or request frame due to lack of check of length of variable received. in Snapdragon Compute, Snapdragon Connectivity in MSM8998, QCA6390, SC7180, SC8180X, SDM850 **CVE ID : CVE-2020-3652**	https://www.qualcomm.com/company/product-security/bulletins/april-2020-bulletin	O-QUA-SDM8-010520/274
Out-of-bounds Read	16-04-2020	9.4	Possible buffer over-read in windows wlan driver function due to lack of check of length of variable received from userspace in Snapdragon Compute,	https://www.qualcomm.com/company/product-security/bulletins/april-	O-QUA-SDM8-010520/275

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Snapdragon Connectivity in MSM8998, QCA6390, SC7180, SC8180X, SDM850 **CVE ID : CVE-2020-3653**	2020-bulletin	
qcm2150_firmware					
Reachable Assertion	16-04-2020	7.8	Active command timeout since WM status change cmd is not removed from active queue if peer sends multiple deauth frames. in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables in APQ8009, APQ8017, APQ8053, APQ8096AU, MDM9206, MDM9207C, MDM9607, MDM9640, MDM9650, MSM8905, MSM8909W, MSM8917, MSM8920, MSM8937, MSM8940, MSM8953, MSM8996AU, QCA6174A, QCA6574AU, QCA9377, QCA9379, QCM2150, QCN7605, QCS605, QM215, SC8180X, SDM429, SDM429W, SDM439, SDM450, SDM630, SDM632, SDM636, SDM660, SDM845, SDX20, SDX24, SDX55, SM8150,	https://www.qualcomm.com/company/product-security/bulletins/april-2020-bulletin	O-QUA-QCM2-010520/276

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			SXR1130 **CVE ID : CVE-2020-3651**		
sdx55_firmware					
Reachable Assertion	16-04-2020	7.8	Active command timeout since WM status change cmd is not removed from active queue if peer sends multiple deauth frames. in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables in APQ8009, APQ8017, APQ8053, APQ8096AU, MDM9206, MDM9207C, MDM9607, MDM9640, MDM9650, MSM8905, MSM8909W, MSM8917, MSM8920, MSM8937, MSM8940, MSM8953, MSM8996AU, QCA6174A, QCA6574AU, QCA9377, QCA9379, QCM2150, QCN7605, QCS605, QM215, SC8180X, SDM429, SDM429W, SDM439, SDM450, SDM630, SDM632, SDM636, SDM660, SDM845, SDX20, SDX24, SDX55, SM8150, SXR1130 **CVE ID : CVE-2020-3651**	https://www.qualcomm.com/company/product-security/bulletins/april-2020-bulletin	O-QUA-SDX5-010520/277

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
sdm439_firmware					
Reachable Assertion	16-04-2020	7.8	Active command timeout since WM status change cmd is not removed from active queue if peer sends multiple deauth frames. in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables in APQ8009, APQ8017, APQ8053, APQ8096AU, MDM9206, MDM9207C, MDM9607, MDM9640, MDM9650, MSM8905, MSM8909W, MSM8917, MSM8920, MSM8937, MSM8940, MSM8953, MSM8996AU, QCA6174A, QCA6574AU, QCA9377, QCA9379, QCM2150, QCN7605, QCS605, QM215, SC8180X, SDM429, SDM429W, SDM439, SDM450, SDM630, SDM632, SDM636, SDM660, SDM845, SDX20, SDX24, SDX55, SM8150, SXR1130 **CVE ID : CVE-2020-3651**	https://www.qualcomm.com/company/product-security/bulletins/april-2020-bulletin	O-QUA-SDM4-010520/278
sdm630_firmware					
Reachable Assertion	16-04-2020	7.8	Active command timeout since WM status change	https://www.qualcomm.	O-QUA-SDM6-

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			cmd is not removed from active queue if peer sends multiple deauth frames. in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables in APQ8009, APQ8017, APQ8053, APQ8096AU, MDM9206, MDM9207C, MDM9607, MDM9640, MDM9650, MSM8905, MSM8909W, MSM8917, MSM8920, MSM8937, MSM8940, MSM8953, MSM8996AU, QCA6174A, QCA6574AU, QCA9377, QCA9379, QCM2150, QCN7605, QCS605, QM215, SC8180X, SDM429, SDM429W, SDM439, SDM450, SDM630, SDM632, SDM636, SDM660, SDM845, SDX20, SDX24, SDX55, SM8150, SXR1130 **CVE ID : CVE-2020-3651**	com/company/product-security/bulletins/april-2020-bulletin	010520/279
sdm660_firmware					
Reachable Assertion	16-04-2020	7.8	Active command timeout since WM status change cmd is not removed from active queue if peer sends multiple deauth frames. in	https://www.qualcomm.com/company/product-security/bull	O-QUA-SDM6-010520/280

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables in APQ8009, APQ8017, APQ8053, APQ8096AU, MDM9206, MDM9207C, MDM9607, MDM9640, MDM9650, MSM8905, MSM8909W, MSM8917, MSM8920, MSM8937, MSM8940, MSM8953, MSM8996AU, QCA6174A, QCA6574AU, QCA9377, QCA9379, QCM2150, QCN7605, QCS605, QM215, SC8180X, SDM429, SDM429W, SDM439, SDM450, SDM630, SDM632, SDM636, SDM660, SDM845, SDX20, SDX24, SDX55, SM8150, SXR1130 **CVE ID : CVE-2020-3651**	etins/april-2020-bulletin	
mdm9640_firmware					
Reachable Assertion	16-04-2020	7.8	Active command timeout since WM status change cmd is not removed from active queue if peer sends multiple deauth frames. in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer	https://www.qualcomm.com/company/product-security/bulletins/april-2020-bulletin	O-QUA-MDM9-010520/281

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables in APQ8009, APQ8017, APQ8053, APQ8096AU, MDM9206, MDM9207C, MDM9607, MDM9640, MDM9650, MSM8905, MSM8909W, MSM8917, MSM8920, MSM8937, MSM8940, MSM8953, MSM8996AU, QCA6174A, QCA6574AU, QCA9377, QCA9379, QCM2150, QCN7605, QCS605, QM215, SC8180X, SDM429, SDM429W, SDM439, SDM450, SDM630, SDM632, SDM636, SDM660, SDM845, SDX20, SDX24, SDX55, SM8150, SXR1130 **CVE ID : CVE-2020-3651**		
msm8909w_firmware					
Reachable Assertion	16-04-2020	7.8	Active command timeout since WM status change cmd is not removed from active queue if peer sends multiple deauth frames. in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon	https://www.qualcomm.com/company/product-security/bulletins/april-2020-bulletin	O-QUA-MSM8-010520/282

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables in APQ8009, APQ8017, APQ8053, APQ8096AU, MDM9206, MDM9207C, MDM9607, MDM9640, MDM9650, MSM8905, MSM8909W, MSM8917, MSM8920, MSM8937, MSM8940, MSM8953, MSM8996AU, QCA6174A, QCA6574AU, QCA9377, QCA9379, QCM2150, QCN7605, QCS605, QM215, SC8180X, SDM429, SDM429W, SDM439, SDM450, SDM630, SDM632, SDM636, SDM660, SDM845, SDX20, SDX24, SDX55, SM8150, SXR1130 **CVE ID : CVE-2020-3651**		
qcs605_firmware					
Reachable Assertion	16-04-2020	7.8	Active command timeout since WM status change cmd is not removed from active queue if peer sends multiple deauth frames. in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice &	https://www.qualcomm.com/company/product-security/bulletins/april-2020-bulletin	O-QUA-QCS6-010520/283

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Music, Snapdragon Wearables in APQ8009, APQ8017, APQ8053, APQ8096AU, MDM9206, MDM9207C, MDM9607, MDM9640, MDM9650, MSM8905, MSM8909W, MSM8917, MSM8920, MSM8937, MSM8940, MSM8953, MSM8996AU, QCA6174A, QCA6574AU, QCA9377, QCA9379, QCM2150, QCN7605, QCS605, QM215, SC8180X, SDM429, SDM429W, SDM439, SDM450, SDM630, SDM632, SDM636, SDM660, SDM845, SDX20, SDX24, SDX55, SM8150, SXR1130 **CVE ID : CVE-2020-3651**		
sdx20_firmware					
Reachable Assertion	16-04-2020	7.8	Active command timeout since WM status change cmd is not removed from active queue if peer sends multiple deauth frames. in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables in APQ8009, APQ8017, APQ8053,	https://www.qualcomm.com/company/product-security/bulletins/april-2020-bulletin	O-QUA-SDX2-010520/284

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			APQ8096AU, MDM9206, MDM9207C, MDM9607, MDM9640, MDM9650, MSM8905, MSM8909W, MSM8917, MSM8920, MSM8937, MSM8940, MSM8953, MSM8996AU, QCA6174A, QCA6574AU, QCA9377, QCA9379, QCM2150, QCN7605, QCS605, QM215, SC8180X, SDM429, SDM429W, SDM439, SDM450, SDM630, SDM632, SDM636, SDM660, SDM845, SDX20, SDX24, SDX55, SM8150, SXR1130 **CVE ID : CVE-2020-3651**		
sxr1130_firmware					
Reachable Assertion	16-04-2020	7.8	Active command timeout since WM status change cmd is not removed from active queue if peer sends multiple deauth frames. in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables in APQ8009, APQ8017, APQ8053, APQ8096AU, MDM9206, MDM9207C, MDM9607, MDM9640, MDM9650,	https://www.qualcomm.com/company/product-security/bulletins/april-2020-bulletin	O-QUA-SXR1-010520/285

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			MSM8905, MSM8909W, MSM8917, MSM8920, MSM8937, MSM8940, MSM8953, MSM8996AU, QCA6174A, QCA6574AU, QCA9377, QCA9379, QCM2150, QCN7605, QCS605, QM215, SC8180X, SDM429, SDM429W, SDM439, SDM450, SDM630, SDM632, SDM636, SDM660, SDM845, SDX20, SDX24, SDX55, SM8150, SXR1130 **CVE ID : CVE-2020-3651**		
sdx24_firmware					
Reachable Assertion	16-04-2020	7.8	Active command timeout since WM status change cmd is not removed from active queue if peer sends multiple deauth frames. in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables in APQ8009, APQ8017, APQ8053, APQ8096AU, MDM9206, MDM9207C, MDM9607, MDM9640, MDM9650, MSM8905, MSM8909W, MSM8917, MSM8920, MSM8937, MSM8940,	https://www.qualcomm.com/company/product-security/bulletins/april-2020-bulletin	O-QUA-SDX2-010520/286

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			MSM8953, MSM8996AU, QCA6174A, QCA6574AU, QCA9377, QCA9379, QCM2150, QCN7605, QCS605, QM215, SC8180X, SDM429, SDM429W, SDM439, SDM450, SDM630, SDM632, SDM636, SDM660, SDM845, SDX20, SDX24, SDX55, SM8150, SXR1130 **CVE ID : CVE-2020-3651**		
qca6390_firmware					
Out-of-bounds Read	16-04-2020	9.4	Possible buffer over-read issue in windows x86 wlan driver function while processing beacon or request frame due to lack of check of length of variable received. in Snapdragon Compute, Snapdragon Connectivity in MSM8998, QCA6390, SC7180, SC8180X, SDM850 **CVE ID : CVE-2020-3652**	https://www.qualcomm.com/company/product-security/bulletins/april-2020-bulletin	O-QUA-QCA6-010520/287
Out-of-bounds Read	16-04-2020	9.4	Possible buffer over-read in windows wlan driver function due to lack of check of length of variable received from userspace in Snapdragon Compute, Snapdragon Connectivity in MSM8998, QCA6390, SC7180, SC8180X, SDM850 **CVE ID : CVE-2020-3653**	https://www.qualcomm.com/company/product-security/bulletins/april-2020-bulletin	O-QUA-QCA6-010520/288
Redhat					

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
enterprise_linux					
Uncontrolled Resource Consumption	17-04-2020	5	ntpd in ntp before 4.2.8p14 and 4.3.x before 4.3.100 allows an off-path attacker to block unauthenticated synchronization via a server mode packet with a spoofed source IP address, because transmissions are rescheduled even when a packet lacks a valid origin timestamp. **CVE ID : CVE-2020-11868**	https://security.netapp.com/advisory/ntap-20200424-0002/	O-RED-ENTE-010520/289
se					
tricon_tcm_4351_firmware					
Uncontrolled Resource Consumption	16-04-2020	5	**VERSION NOT SUPPORTED WHEN ASSIGNED** A vulnerability could cause TCM modules to reset when under high network load in TCM v10.4.x and in system v10.3.x. This vulnerability was discovered and remediated in version v10.5.x on August 13, 2009. TCMs from v10.5.x and on will no longer exhibit this behavior. **CVE ID : CVE-2020-7486**	N/A	O-SE-TRIC-010520/290
tricon_tcm_4352_firmware					
Uncontrolled Resource Consumption	16-04-2020	5	**VERSION NOT SUPPORTED WHEN ASSIGNED** A vulnerability could cause	N/A	O-SE-TRIC-010520/291

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			TCM modules to reset when under high network load in TCM v10.4.x and in system v10.3.x. This vulnerability was discovered and remediated in version v10.5.x on August 13, 2009. TCMs from v10.5.x and on will no longer exhibit this behavior. **CVE ID : CVE-2020-7486**		
tricon_tcm_4351a_firmware					
Uncontrolled Resource Consumption	16-04-2020	5	**VERSION NOT SUPPORTED WHEN ASSIGNED** A vulnerability could cause TCM modules to reset when under high network load in TCM v10.4.x and in system v10.3.x. This vulnerability was discovered and remediated in version v10.5.x on August 13, 2009. TCMs from v10.5.x and on will no longer exhibit this behavior. **CVE ID : CVE-2020-7486**	N/A	O-SE-TRIC-010520/292
tricon_tcm_4351b_firmware					
Uncontrolled Resource Consumption	16-04-2020	5	**VERSION NOT SUPPORTED WHEN ASSIGNED** A vulnerability could cause TCM modules to reset when under high network load in TCM v10.4.x and in system v10.3.x. This vulnerability was	N/A	O-SE-TRIC-010520/293

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			discovered and remediated in version v10.5.x on August 13, 2009. TCMs from v10.5.x and on will no longer exhibit this behavior. **CVE ID : CVE-2020-7486**		
tricon_tcm_4352a_firmware					
Uncontrolled Resource Consumption	16-04-2020	5	**VERSION NOT SUPPORTED WHEN ASSIGNED** A vulnerability could cause TCM modules to reset when under high network load in TCM v10.4.x and in system v10.3.x. This vulnerability was discovered and remediated in version v10.5.x on August 13, 2009. TCMs from v10.5.x and on will no longer exhibit this behavior. **CVE ID : CVE-2020-7486**	N/A	O-SE-TRIC-010520/294
tricon_tcm_4352b_firmware					
Uncontrolled Resource Consumption	16-04-2020	5	**VERSION NOT SUPPORTED WHEN ASSIGNED** A vulnerability could cause TCM modules to reset when under high network load in TCM v10.4.x and in system v10.3.x. This vulnerability was discovered and remediated in version v10.5.x on August 13, 2009. TCMs from v10.5.x and on will no longer	N/A	O-SE-TRIC-010520/295

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			exhibit this behavior. **CVE ID : CVE-2020-7486**		
modicon_m218_firmware					
Insufficient Verification of Data Authenticity	22-04-2020	7.5	A CWE-345: Insufficient Verification of Data Authenticity vulnerability exists which could allow the attacker to execute malicious code on the Modicon M218, M241, M251, and M258 controllers. **CVE ID : CVE-2020-7487**	N/A	O-SE-MODI-010520/296
Cleartext Transmission of Sensitive Information	22-04-2020	5	A CWE-319: Cleartext Transmission of Sensitive Information vulnerability exists which could leak sensitive information transmitted between the software and the Modicon M218, M241, M251, and M258 controllers. **CVE ID : CVE-2020-7488**	N/A	O-SE-MODI-010520/297
modicon_m241_firmware					
Insufficient Verification of Data Authenticity	22-04-2020	7.5	A CWE-345: Insufficient Verification of Data Authenticity vulnerability exists which could allow the attacker to execute malicious code on the Modicon M218, M241, M251, and M258 controllers. **CVE ID : CVE-2020-7487**	N/A	O-SE-MODI-010520/298
Cleartext Transmission of Sensitive Information	22-04-2020	5	A CWE-319: Cleartext Transmission of Sensitive Information vulnerability exists which could leak	N/A	O-SE-MODI-010520/299

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			sensitive information transmitted between the software and the Modicon M218, M241, M251, and M258 controllers. **CVE ID : CVE-2020-7488**		
modicon_m251_firmware					
Insufficient Verification of Data Authenticity	22-04-2020	7.5	A CWE-345: Insufficient Verification of Data Authenticity vulnerability exists which could allow the attacker to execute malicious code on the Modicon M218, M241, M251, and M258 controllers. **CVE ID : CVE-2020-7487**	N/A	O-SE-MODI-010520/300
Cleartext Transmission of Sensitive Information	22-04-2020	5	A CWE-319: Cleartext Transmission of Sensitive Information vulnerability exists which could leak sensitive information transmitted between the software and the Modicon M218, M241, M251, and M258 controllers. **CVE ID : CVE-2020-7488**	N/A	O-SE-MODI-010520/301
modicon_m258_firmware					
Insufficient Verification of Data Authenticity	22-04-2020	7.5	A CWE-345: Insufficient Verification of Data Authenticity vulnerability exists which could allow the attacker to execute malicious code on the Modicon M218, M241, M251, and M258 controllers. **CVE ID : CVE-2020-7487**	N/A	O-SE-MODI-010520/302

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Cleartext Transmission of Sensitive Information	22-04-2020	5	A CWE-319: Cleartext Transmission of Sensitive Information vulnerability exists which could leak sensitive information transmitted between the software and the Modicon M218, M241, M251, and M258 controllers. **CVE ID : CVE-2020-7488**	N/A	O-SE-MODI-010520/303
Windriver					
vxworks					
NULL Pointer Dereference	27-04-2020	5	The IGMP component in VxWorks 6.8.3 IPNET CVE patches created in 2019 has a NULL Pointer Dereference. **CVE ID : CVE-2020-10664**	https://support2.windriver.com/index.php?page=cve&on=view&id=CVE-2020-10664	O-WIN-VXWO-010520/304
Hardware					
Dlink					
dsl-2640b					
Insufficiently Protected Credentials	20-04-2020	5	An issue was discovered on D-Link DSL-2640B B2 EU_4.01B devices. A cfm UDP service listening on port 65002 allows remote, unauthenticated exfiltration of administrative credentials. **CVE ID : CVE-2020-9275**	N/A	H-DLI-DSL--010520/305
Out-of-bounds Write	20-04-2020	9	An issue was discovered on D-Link DSL-2640B B2 EU_4.01B devices. The function do_cgi(), which processes cgi requests supplied to the device's	N/A	H-DLI-DSL--010520/306

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			web servers, is vulnerable to a remotely exploitable stack-based buffer overflow. Unauthenticated exploitation is possible by combining this vulnerability with CVE-2020-9277. **CVE ID : CVE-2020-9276**		
Improper Authentication	20-04-2020	7.5	An issue was discovered on D-Link DSL-2640B B2 EU_4.01B devices. Authentication can be bypassed when accessing cgi modules. This allows one to perform administrative tasks (e.g., modify the admin password) with no authentication. **CVE ID : CVE-2020-9277**	N/A	H-DLI-DSL--010520/307
Improper Input Validation	20-04-2020	6.4	An issue was discovered on D-Link DSL-2640B B2 EU_4.01B devices. The device can be reset to its default configuration by accessing an unauthenticated URL. **CVE ID : CVE-2020-9278**	N/A	H-DLI-DSL--010520/308
Use of Hard-coded Credentials	20-04-2020	10	An issue was discovered on D-Link DSL-2640B B2 EU_4.01B devices. A hard-coded account allows management-interface login with high privileges. The logged-in user can perform critical tasks and take full control of the	N/A	H-DLI-DSL--010520/309

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			device. **CVE ID : CVE-2020-9279**		
evenroute					
iqrouter					
Improper Neutralization of Special Elements used in an OS Command ('OS Command Injection')	21-04-2020	7.5	IQrouter through 3.3.1, when unconfigured, has multiple remote code execution vulnerabilities in the web-panel because of Bash Shell Metacharacter Injection. **CVE ID : CVE-2020-11963**	N/A	H-EVE-IQRO-010520/310
Insufficiently Protected Credentials	21-04-2020	5	In IQrouter through 3.3.1, the Lua function diag_set_password in the web-panel allows remote attackers to change the root password arbitrarily. **CVE ID : CVE-2020-11964**	N/A	H-EVE-IQRO-010520/311
Insufficiently Protected Credentials	21-04-2020	7.5	In IQrouter through 3.3.1, there is a root user without a password, which allows attackers to gain full remote access via SSH. **CVE ID : CVE-2020-11965**	N/A	H-EVE-IQRO-010520/312
Weak Password Requirements	21-04-2020	7.5	In IQrouter through 3.3.1, the Lua function reset_password in the web-panel allows remote attackers to change the root password arbitrarily. **CVE ID : CVE-2020-11966**	N/A	H-EVE-IQRO-010520/313

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Improper Privilege Management	21-04-2020	9	In IQrouter through 3.3.1, remote attackers can control the device (restart network, reboot, upgrade, reset) because of Incorrect Access Control. **CVE ID : CVE-2020-11967**	N/A	H-EVE-IQRO-010520/314
Information Exposure Through Log Files	21-04-2020	5	In the web-panel in IQrouter through 3.3.1, remote attackers can read system logs because of Incorrect Access Control. **CVE ID : CVE-2020-11968**	N/A	H-EVE-IQRO-010520/315
Huawei					
honor_v20					
Information Exposure	20-04-2020	2.9	Huawei smartphones Honor V20 with versions earlier than 10.0.0.179(C636E3R4P3), versions earlier than 10.0.0.180(C185E3R3P3), versions earlier than 10.0.0.180(C432E10R3P4) have an information disclosure vulnerability. The device does not sufficiently validate the identity of smart wearable device in certain specific scenario, the attacker need to gain certain information in the victim's smartphone to launch the attack, successful exploit could cause information disclosure.	http://www.huawei.com/en/psirt/security-advisories/huawei-sa-20200415-02-smartphone-en, https://www.huawei.com/en/psirt/security-advisories/huawei-sa-20200415-02-smartphone-en	H-HUA-HONO-010520/316

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2020-1803		
taurus-al00b					
Information Exposure	20-04-2020	4.3	Huawei smartphones Taurus-AL00B with versions earlier than 10.0.0.205(C00E201R7P2) have an improper authentication vulnerability. The software insufficiently validate the user's identity when a user wants to do certain operation. An attacker can trick user into installing a malicious application to exploit this vulnerability. Successful exploit may cause some information disclosure. **CVE ID : CVE-2020-9070**	http://www.huawei.com/en/psirt/security-advisories/huawei-sa-20200415-01-smartphone-en, https://www.huawei.com/en/psirt/security-advisories/huawei-sa-20200415-01-smartphone-en	H-HUA-TAUR-010520/317
Qualcomm					
mdm9206					
Reachable Assertion	16-04-2020	7.8	Active command timeout since WM status change cmd is not removed from active queue if peer sends multiple deauth frames. in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables in APQ8009,	https://www.qualcomm.com/company/product-security/bulletins/april-2020-bulletin	H-QUA-MDM9-010520/318

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			APQ8017, APQ8053, APQ8096AU, MDM9206, MDM9207C, MDM9607, MDM9640, MDM9650, MSM8905, MSM8909W, MSM8917, MSM8920, MSM8937, MSM8940, MSM8953, MSM8996AU, QCA6174A, QCA6574AU, QCA9377, QCA9379, QCM2150, QCN7605, QCS605, QM215, SC8180X, SDM429, SDM429W, SDM439, SDM450, SDM630, SDM632, SDM636, SDM660, SDM845, SDX20, SDX24, SDX55, SM8150, SXR1130 **CVE ID : CVE-2020-3651**		
mdm9607					
Reachable Assertion	16-04-2020	7.8	Active command timeout since WM status change cmd is not removed from active queue if peer sends multiple deauth frames. in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables in APQ8009, APQ8017, APQ8053, APQ8096AU, MDM9206, MDM9207C, MDM9607,	https://www.qualcomm.com/company/product-security/bulletins/april-2020-bulletin	H-QUA-MDM9-010520/319

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			MDM9640, MDM9650, MSM8905, MSM8909W, MSM8917, MSM8920, MSM8937, MSM8940, MSM8953, MSM8996AU, QCA6174A, QCA6574AU, QCA9377, QCA9379, QCM2150, QCN7605, QCS605, QM215, SC8180X, SDM429, SDM429W, SDM439, SDM450, SDM630, SDM632, SDM636, SDM660, SDM845, SDX20, SDX24, SDX55, SM8150, SXR1130 **CVE ID : CVE-2020-3651**		
msm8909w					
Reachable Assertion	16-04-2020	7.8	Active command timeout since WM status change cmd is not removed from active queue if peer sends multiple deauth frames. in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables in APQ8009, APQ8017, APQ8053, APQ8096AU, MDM9206, MDM9207C, MDM9607, MDM9640, MDM9650, MSM8905, MSM8909W, MSM8917, MSM8920,	https://www.qualcomm.com/company/product-security/bulletins/april-2020-bulletin	H-QUA-MSM8-010520/320

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			MSM8937, MSM8940, MSM8953, MSM8996AU, QCA6174A, QCA6574AU, QCA9377, QCA9379, QCM2150, QCN7605, QCS605, QM215, SC8180X, SDM429, SDM429W, SDM439, SDM450, SDM630, SDM632, SDM636, SDM660, SDM845, SDX20, SDX24, SDX55, SM8150, SXR1130 **CVE ID : CVE-2020-3651**		
msm8996au					
Reachable Assertion	16-04-2020	7.8	Active command timeout since WM status change cmd is not removed from active queue if peer sends multiple deauth frames. in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables in APQ8009, APQ8017, APQ8053, APQ8096AU, MDM9206, MDM9207C, MDM9607, MDM9640, MDM9650, MSM8905, MSM8909W, MSM8917, MSM8920, MSM8937, MSM8940, MSM8953, MSM8996AU, QCA6174A, QCA6574AU,	https://www.qualcomm.com/company/product-security/bulletins/april-2020-bulletin	H-QUA-MSM8-010520/321

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			QCA9377, QCA9379, QCM2150, QCN7605, QCS605, QM215, SC8180X, SDM429, SDM429W, SDM439, SDM450, SDM630, SDM632, SDM636, SDM660, SDM845, SDX20, SDX24, SDX55, SM8150, SXR1130 **CVE ID : CVE-2020-3651**		
qca6574au					
Reachable Assertion	16-04-2020	7.8	Active command timeout since WM status change cmd is not removed from active queue if peer sends multiple deauth frames. in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables in APQ8009, APQ8017, APQ8053, APQ8096AU, MDM9206, MDM9207C, MDM9607, MDM9640, MDM9650, MSM8905, MSM8909W, MSM8917, MSM8920, MSM8937, MSM8940, MSM8953, MSM8996AU, QCA6174A, QCA6574AU, QCA9377, QCA9379, QCM2150, QCN7605, QCS605, QM215,	https://www.qualcomm.com/company/product-security/bulletins/april-2020-bulletin	H-QUA-QCA6-010520/322

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			SC8180X, SDM429, SDM429W, SDM439, SDM450, SDM630, SDM632, SDM636, SDM660, SDM845, SDX20, SDX24, SDX55, SM8150, SXR1130 **CVE ID : CVE-2020-3651**		
qcs605					
Reachable Assertion	16-04-2020	7.8	Active command timeout since WM status change cmd is not removed from active queue if peer sends multiple deauth frames. in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables in APQ8009, APQ8017, APQ8053, APQ8096AU, MDM9206, MDM9207C, MDM9607, MDM9640, MDM9650, MSM8905, MSM8909W, MSM8917, MSM8920, MSM8937, MSM8940, MSM8953, MSM8996AU, QCA6174A, QCA6574AU, QCA9377, QCA9379, QCM2150, QCN7605, QCS605, QM215, SC8180X, SDM429, SDM429W, SDM439, SDM450, SDM630,	https://www.qualcomm.com/company/product-security/bulletins/april-2020-bulletin	H-QUA-QCS6-010520/323

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			SDM632, SDM636, SDM660, SDM845, SDX20, SDX24, SDX55, SM8150, SXR1130 **CVE ID : CVE-2020-3651**		
sdm439					
Reachable Assertion	16-04-2020	7.8	Active command timeout since WM status change cmd is not removed from active queue if peer sends multiple deauth frames. in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables in APQ8009, APQ8017, APQ8053, APQ8096AU, MDM9206, MDM9207C, MDM9607, MDM9640, MDM9650, MSM8905, MSM8909W, MSM8917, MSM8920, MSM8937, MSM8940, MSM8953, MSM8996AU, QCA6174A, QCA6574AU, QCA9377, QCA9379, QCM2150, QCN7605, QCS605, QM215, SC8180X, SDM429, SDM429W, SDM439, SDM450, SDM630, SDM632, SDM636, SDM660, SDM845, SDX20, SDX24, SDX55, SM8150,	https://www.qualcomm.com/company/product-security/bulletins/april-2020-bulletin	H-QUA-SDM4-010520/324

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			SXR1130 **CVE ID : CVE-2020-3651**		
sdm630					
Reachable Assertion	16-04-2020	7.8	Active command timeout since WM status change cmd is not removed from active queue if peer sends multiple deauth frames. in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables in APQ8009, APQ8017, APQ8053, APQ8096AU, MDM9206, MDM9207C, MDM9607, MDM9640, MDM9650, MSM8905, MSM8909W, MSM8917, MSM8920, MSM8937, MSM8940, MSM8953, MSM8996AU, QCA6174A, QCA6574AU, QCA9377, QCA9379, QCM2150, QCN7605, QCS605, QM215, SC8180X, SDM429, SDM429W, SDM439, SDM450, SDM630, SDM632, SDM636, SDM660, SDM845, SDX20, SDX24, SDX55, SM8150, SXR1130 **CVE ID : CVE-2020-3651**	https://www.qualcomm.com/company/product-security/bulletins/april-2020-bulletin	H-QUA-SDM6-010520/325

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
sdm660					
Reachable Assertion	16-04-2020	7.8	Active command timeout since WM status change cmd is not removed from active queue if peer sends multiple deauth frames. in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables in APQ8009, APQ8017, APQ8053, APQ8096AU, MDM9206, MDM9207C, MDM9607, MDM9640, MDM9650, MSM8905, MSM8909W, MSM8917, MSM8920, MSM8937, MSM8940, MSM8953, MSM8996AU, QCA6174A, QCA6574AU, QCA9377, QCA9379, QCM2150, QCN7605, QCS605, QM215, SC8180X, SDM429, SDM429W, SDM439, SDM450, SDM630, SDM632, SDM636, SDM660, SDM845, SDX20, SDX24, SDX55, SM8150, SXR1130 **CVE ID : CVE-2020-3651**	https://www.qualcomm.com/company/product-security/bulletins/april-2020-bulletin	H-QUA-SDM6-010520/326
sdx20					
Reachable Assertion	16-04-2020	7.8	Active command timeout since WM status change	https://www.qualcomm.	H-QUA-SDX2-

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			cmd is not removed from active queue if peer sends multiple deauth frames. in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables in APQ8009, APQ8017, APQ8053, APQ8096AU, MDM9206, MDM9207C, MDM9607, MDM9640, MDM9650, MSM8905, MSM8909W, MSM8917, MSM8920, MSM8937, MSM8940, MSM8953, MSM8996AU, QCA6174A, QCA6574AU, QCA9377, QCA9379, QCM2150, QCN7605, QCS605, QM215, SC8180X, SDM429, SDM429W, SDM439, SDM450, SDM630, SDM632, SDM636, SDM660, SDM845, SDX20, SDX24, SDX55, SM8150, SXR1130 **CVE ID : CVE-2020-3651**	com/company/product-security/bulletins/april-2020-bulletin	010520/327
mdm9640					
Reachable Assertion	16-04-2020	7.8	Active command timeout since WM status change cmd is not removed from active queue if peer sends multiple deauth frames. in	https://www.qualcomm.com/company/product-security/bull	H-QUA-MDM9-010520/328

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables in APQ8009, APQ8017, APQ8053, APQ8096AU, MDM9206, MDM9207C, MDM9607, MDM9640, MDM9650, MSM8905, MSM8909W, MSM8917, MSM8920, MSM8937, MSM8940, MSM8953, MSM8996AU, QCA6174A, QCA6574AU, QCA9377, QCA9379, QCM2150, QCN7605, QCS605, QM215, SC8180X, SDM429, SDM429W, SDM439, SDM450, SDM630, SDM632, SDM636, SDM660, SDM845, SDX20, SDX24, SDX55, SM8150, SXR1130 **CVE ID : CVE-2020-3651**	etins/april-2020-bulletin	
mdm9650					
Reachable Assertion	16-04-2020	7.8	Active command timeout since WM status change cmd is not removed from active queue if peer sends multiple deauth frames. in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer	https://www.qualcomm.com/company/product-security/bulletins/april-2020-bulletin	H-QUA-MDM9-010520/329

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables in APQ8009, APQ8017, APQ8053, APQ8096AU, MDM9206, MDM9207C, MDM9607, MDM9640, MDM9650, MSM8905, MSM8909W, MSM8917, MSM8920, MSM8937, MSM8940, MSM8953, MSM8996AU, QCA6174A, QCA6574AU, QCA9377, QCA9379, QCM2150, QCN7605, QCS605, QM215, SC8180X, SDM429, SDM429W, SDM439, SDM450, SDM630, SDM632, SDM636, SDM660, SDM845, SDX20, SDX24, SDX55, SM8150, SXR1130 **CVE ID : CVE-2020-3651**		
sdx24					
Reachable Assertion	16-04-2020	7.8	Active command timeout since WM status change cmd is not removed from active queue if peer sends multiple deauth frames. in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon	https://www.qualcomm.com/company/product-security/bulletins/april-2020-bulletin	H-QUA-SDX2-010520/330

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables in APQ8009, APQ8017, APQ8053, APQ8096AU, MDM9206, MDM9207C, MDM9607, MDM9640, MDM9650, MSM8905, MSM8909W, MSM8917, MSM8920, MSM8937, MSM8940, MSM8953, MSM8996AU, QCA6174A, QCA6574AU, QCA9377, QCA9379, QCM2150, QCN7605, QCS605, QM215, SC8180X, SDM429, SDM429W, SDM439, SDM450, SDM630, SDM632, SDM636, SDM660, SDM845, SDX20, SDX24, SDX55, SM8150, SXR1130 **CVE ID : CVE-2020-3651**		
qca6174a					
Reachable Assertion	16-04-2020	7.8	Active command timeout since WM status change cmd is not removed from active queue if peer sends multiple deauth frames. in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice &	https://www.qualcomm.com/company/product-security/bulletins/april-2020-bulletin	H-QUA-QCA6-010520/331

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Music, Snapdragon Wearables in APQ8009, APQ8017, APQ8053, APQ8096AU, MDM9206, MDM9207C, MDM9607, MDM9640, MDM9650, MSM8905, MSM8909W, MSM8917, MSM8920, MSM8937, MSM8940, MSM8953, MSM8996AU, QCA6174A, QCA6574AU, QCA9377, QCA9379, QCM2150, QCN7605, QCS605, QM215, SC8180X, SDM429, SDM429W, SDM439, SDM450, SDM630, SDM632, SDM636, SDM660, SDM845, SDX20, SDX24, SDX55, SM8150, SXR1130 **CVE ID : CVE-2020-3651**		
qca9377					
Reachable Assertion	16-04-2020	7.8	Active command timeout since WM status change cmd is not removed from active queue if peer sends multiple deauth frames. in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables in APQ8009, APQ8017, APQ8053,	https://www.qualcomm.com/company/product-security/bulletins/april-2020-bulletin	H-QUA-QCA9-010520/332

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			APQ8096AU, MDM9206, MDM9207C, MDM9607, MDM9640, MDM9650, MSM8905, MSM8909W, MSM8917, MSM8920, MSM8937, MSM8940, MSM8953, MSM8996AU, QCA6174A, QCA6574AU, QCA9377, QCA9379, QCM2150, QCN7605, QCS605, QM215, SC8180X, SDM429, SDM429W, SDM439, SDM450, SDM630, SDM632, SDM636, SDM660, SDM845, SDX20, SDX24, SDX55, SM8150, SXR1130 **CVE ID : CVE-2020-3651**		
qca9379					
Reachable Assertion	16-04-2020	7.8	Active command timeout since WM status change cmd is not removed from active queue if peer sends multiple deauth frames. in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables in APQ8009, APQ8017, APQ8053, APQ8096AU, MDM9206, MDM9207C, MDM9607, MDM9640, MDM9650,	https://www.qualcomm.com/company/product-security/bulletins/april-2020-bulletin	H-QUA-QCA9-010520/333

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			MSM8905, MSM8909W, MSM8917, MSM8920, MSM8937, MSM8940, MSM8953, MSM8996AU, QCA6174A, QCA6574AU, QCA9377, QCA9379, QCM2150, QCN7605, QCS605, QM215, SC8180X, SDM429, SDM429W, SDM439, SDM450, SDM630, SDM632, SDM636, SDM660, SDM845, SDX20, SDX24, SDX55, SM8150, SXR1130 **CVE ID : CVE-2020-3651**		
sdm429w					
Reachable Assertion	16-04-2020	7.8	Active command timeout since WM status change cmd is not removed from active queue if peer sends multiple deauth frames. in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables in APQ8009, APQ8017, APQ8053, APQ8096AU, MDM9206, MDM9207C, MDM9607, MDM9640, MDM9650, MSM8905, MSM8909W, MSM8917, MSM8920, MSM8937, MSM8940,	https://www.qualcomm.com/company/product-security/bulletins/april-2020-bulletin	H-QUA-SDM4-010520/334

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			MSM8953, MSM8996AU, QCA6174A, QCA6574AU, QCA9377, QCA9379, QCM2150, QCN7605, QCS605, QM215, SC8180X, SDM429, SDM429W, SDM439, SDM450, SDM630, SDM632, SDM636, SDM660, SDM845, SDX20, SDX24, SDX55, SM8150, SXR1130 **CVE ID : CVE-2020-3651**		
sc7180					
Out-of-bounds Read	16-04-2020	9.4	Possible buffer over-read issue in windows x86 wlan driver function while processing beacon or request frame due to lack of check of length of variable received. in Snapdragon Compute, Snapdragon Connectivity in MSM8998, QCA6390, SC7180, SC8180X, SDM850 **CVE ID : CVE-2020-3652**	https://www.qualcomm.com/company/product-security/bulletins/april-2020-bulletin	H-QUA-SC71-010520/335
Out-of-bounds Read	16-04-2020	9.4	Possible buffer over-read in windows wlan driver function due to lack of check of length of variable received from userspace in Snapdragon Compute, Snapdragon Connectivity in MSM8998, QCA6390, SC7180, SC8180X, SDM850 **CVE ID : CVE-2020-3653**	https://www.qualcomm.com/company/product-security/bulletins/april-2020-bulletin	H-QUA-SC71-010520/336
apq8009					

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Reachable Assertion	16-04-2020	7.8	Active command timeout since WM status change cmd is not removed from active queue if peer sends multiple deauth frames. in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables in APQ8009, APQ8017, APQ8053, APQ8096AU, MDM9206, MDM9207C, MDM9607, MDM9640, MDM9650, MSM8905, MSM8909W, MSM8917, MSM8920, MSM8937, MSM8940, MSM8953, MSM8996AU, QCA6174A, QCA6574AU, QCA9377, QCA9379, QCM2150, QCN7605, QCS605, QM215, SC8180X, SDM429, SDM429W, SDM439, SDM450, SDM630, SDM632, SDM636, SDM660, SDM845, SDX20, SDX24, SDX55, SM8150, SXR1130 **CVE ID : CVE-2020-3651**	https://www.qualcomm.com/company/product-security/bulletins/april-2020-bulletin	H-QUA-APQ8-010520/337
msm8953					
Reachable Assertion	16-04-2020	7.8	Active command timeout since WM status change cmd is not removed from	https://www.qualcomm.com/compan	H-QUA-MSM8-010520/338

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			active queue if peer sends multiple deauth frames. in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables in APQ8009, APQ8017, APQ8053, APQ8096AU, MDM9206, MDM9207C, MDM9607, MDM9640, MDM9650, MSM8905, MSM8909W, MSM8917, MSM8920, MSM8937, MSM8940, MSM8953, MSM8996AU, QCA6174A, QCA6574AU, QCA9377, QCA9379, QCM2150, QCN7605, QCS605, QM215, SC8180X, SDM429, SDM429W, SDM439, SDM450, SDM630, SDM632, SDM636, SDM660, SDM845, SDX20, SDX24, SDX55, SM8150, SXR1130 **CVE ID : CVE-2020-3651**	y/product-security/bulletins/april-2020-bulletin	
msm8998					
Out-of-bounds Read	16-04-2020	9.4	Possible buffer over-read issue in windows x86 wlan driver function while processing beacon or request frame due to lack of check of length of	https://www.qualcomm.com/company/product-security/bulletins/april-	H-QUA-MSM8-010520/339

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			variable received. in Snapdragon Compute, Snapdragon Connectivity in MSM8998, QCA6390, SC7180, SC8180X, SDM850 **CVE ID : CVE-2020-3652**	2020-bulletin	
Out-of-bounds Read	16-04-2020	9.4	Possible buffer over-read in windows wlan driver function due to lack of check of length of variable received from userspace in Snapdragon Compute, Snapdragon Connectivity in MSM8998, QCA6390, SC7180, SC8180X, SDM850 **CVE ID : CVE-2020-3653**	https://www.qualcomm.com/company/product-security/bulletins/april-2020-bulletin	H-QUA-MSM8-010520/340
apq8053					
Reachable Assertion	16-04-2020	7.8	Active command timeout since WM status change cmd is not removed from active queue if peer sends multiple deauth frames. in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables in APQ8009, APQ8017, APQ8053, APQ8096AU, MDM9206, MDM9207C, MDM9607, MDM9640, MDM9650, MSM8905, MSM8909W,	https://www.qualcomm.com/company/product-security/bulletins/april-2020-bulletin	H-QUA-APQ8-010520/341

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			MSM8917, MSM8920, MSM8937, MSM8940, MSM8953, MSM8996AU, QCA6174A, QCA6574AU, QCA9377, QCA9379, QCM2150, QCN7605, QCS605, QM215, SC8180X, SDM429, SDM429W, SDM439, SDM450, SDM630, SDM632, SDM636, SDM660, SDM845, SDX20, SDX24, SDX55, SM8150, SXR1130 **CVE ID : CVE-2020-3651**		
mdm9207c					
Reachable Assertion	16-04-2020	7.8	Active command timeout since WM status change cmd is not removed from active queue if peer sends multiple deauth frames. in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables in APQ8009, APQ8017, APQ8053, APQ8096AU, MDM9206, MDM9207C, MDM9607, MDM9640, MDM9650, MSM8905, MSM8909W, MSM8917, MSM8920, MSM8937, MSM8940, MSM8953, MSM8996AU,	https://www.qualcomm.com/company/product-security/bulletins/april-2020-bulletin	H-QUA-MDM9-010520/342

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			QCA6174A, QCA6574AU, QCA9377, QCA9379, QCM2150, QCN7605, QCS605, QM215, SC8180X, SDM429, SDM429W, SDM439, SDM450, SDM630, SDM632, SDM636, SDM660, SDM845, SDX20, SDX24, SDX55, SM8150, SXR1130 **CVE ID : CVE-2020-3651**		
msm8905					
Reachable Assertion	16-04-2020	7.8	Active command timeout since WM status change cmd is not removed from active queue if peer sends multiple deauth frames. in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables in APQ8009, APQ8017, APQ8053, APQ8096AU, MDM9206, MDM9207C, MDM9607, MDM9640, MDM9650, MSM8905, MSM8909W, MSM8917, MSM8920, MSM8937, MSM8940, MSM8953, MSM8996AU, QCA6174A, QCA6574AU, QCA9377, QCA9379, QCM2150, QCN7605,	https://www.qualcomm.com/company/product-security/bulletins/april-2020-bulletin	H-QUA-MSM8-010520/343

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			QCS605, QM215, SC8180X, SDM429, SDM429W, SDM439, SDM450, SDM630, SDM632, SDM636, SDM660, SDM845, SDX20, SDX24, SDX55, SM8150, SXR1130 **CVE ID : CVE-2020-3651**		
qcn7605					
Reachable Assertion	16-04-2020	7.8	Active command timeout since WM status change cmd is not removed from active queue if peer sends multiple deauth frames. in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables in APQ8009, APQ8017, APQ8053, APQ8096AU, MDM9206, MDM9207C, MDM9607, MDM9640, MDM9650, MSM8905, MSM8909W, MSM8917, MSM8920, MSM8937, MSM8940, MSM8953, MSM8996AU, QCA6174A, QCA6574AU, QCA9377, QCA9379, QCM2150, QCN7605, QCS605, QM215, SC8180X, SDM429, SDM429W, SDM439,	https://www.qualcomm.com/company/product-security/bulletins/april-2020-bulletin	H-QUA-QCN7-010520/344

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			SDM450, SDM630, SDM632, SDM636, SDM660, SDM845, SDX20, SDX24, SDX55, SM8150, SXR1130 **CVE ID : CVE-2020-3651**		
sdm845					
Reachable Assertion	16-04-2020	7.8	Active command timeout since WM status change cmd is not removed from active queue if peer sends multiple deauth frames. in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables in APQ8009, APQ8017, APQ8053, APQ8096AU, MDM9206, MDM9207C, MDM9607, MDM9640, MDM9650, MSM8905, MSM8909W, MSM8917, MSM8920, MSM8937, MSM8940, MSM8953, MSM8996AU, QCA6174A, QCA6574AU, QCA9377, QCA9379, QCM2150, QCN7605, QCS605, QM215, SC8180X, SDM429, SDM429W, SDM439, SDM450, SDM630, SDM632, SDM636, SDM660, SDM845, SDX20,	https://www.qualcomm.com/company/product-security/bulletins/april-2020-bulletin	H-QUA-SDM8-010520/345

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			SDX24, SDX55, SM8150, SXR1130 **CVE ID : CVE-2020-3651**		
apq8017					
Reachable Assertion	16-04-2020	7.8	Active command timeout since WM status change cmd is not removed from active queue if peer sends multiple deauth frames. in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables in APQ8009, APQ8017, APQ8053, APQ8096AU, MDM9206, MDM9207C, MDM9607, MDM9640, MDM9650, MSM8905, MSM8909W, MSM8917, MSM8920, MSM8937, MSM8940, MSM8953, MSM8996AU, QCA6174A, QCA6574AU, QCA9377, QCA9379, QCM2150, QCN7605, QCS605, QM215, SC8180X, SDM429, SDM429W, SDM439, SDM450, SDM630, SDM632, SDM636, SDM660, SDM845, SDX20, SDX24, SDX55, SM8150, SXR1130 **CVE ID : CVE-2020-3651**	https://www.qualcomm.com/company/product-security/bulletins/april-2020-bulletin	H-QUA-APQ8-010520/346

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
apq8096au					
Reachable Assertion	16-04-2020	7.8	Active command timeout since WM status change cmd is not removed from active queue if peer sends multiple deauth frames. in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables in APQ8009, APQ8017, APQ8053, APQ8096AU, MDM9206, MDM9207C, MDM9607, MDM9640, MDM9650, MSM8905, MSM8909W, MSM8917, MSM8920, MSM8937, MSM8940, MSM8953, MSM8996AU, QCA6174A, QCA6574AU, QCA9377, QCA9379, QCM2150, QCN7605, QCS605, QM215, SC8180X, SDM429, SDM429W, SDM439, SDM450, SDM630, SDM632, SDM636, SDM660, SDM845, SDX20, SDX24, SDX55, SM8150, SXR1130 **CVE ID : CVE-2020-3651**	https://www.qualcomm.com/company/product-security/bulletins/april-2020-bulletin	H-QUA-APQ8-010520/347
sdm636					
Reachable Assertion	16-04-2020	7.8	Active command timeout since WM status change	https://www.qualcomm.	H-QUA-SDM6-

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			cmd is not removed from active queue if peer sends multiple deauth frames. in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables in APQ8009, APQ8017, APQ8053, APQ8096AU, MDM9206, MDM9207C, MDM9607, MDM9640, MDM9650, MSM8905, MSM8909W, MSM8917, MSM8920, MSM8937, MSM8940, MSM8953, MSM8996AU, QCA6174A, QCA6574AU, QCA9377, QCA9379, QCM2150, QCN7605, QCS605, QM215, SC8180X, SDM429, SDM429W, SDM439, SDM450, SDM630, SDM632, SDM636, SDM660, SDM845, SDX20, SDX24, SDX55, SM8150, SXR1130 **CVE ID : CVE-2020-3651**	com/company/product-security/bulletins/april-2020-bulletin	010520/348
sxr1130					
Reachable Assertion	16-04-2020	7.8	Active command timeout since WM status change cmd is not removed from active queue if peer sends multiple deauth frames. in	https://www.qualcomm.com/company/product-security/bull	H-QUA-SXR1-010520/349

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables in APQ8009, APQ8017, APQ8053, APQ8096AU, MDM9206, MDM9207C, MDM9607, MDM9640, MDM9650, MSM8905, MSM8909W, MSM8917, MSM8920, MSM8937, MSM8940, MSM8953, MSM8996AU, QCA6174A, QCA6574AU, QCA9377, QCA9379, QCM2150, QCN7605, QCS605, QM215, SC8180X, SDM429, SDM429W, SDM439, SDM450, SDM630, SDM632, SDM636, SDM660, SDM845, SDX20, SDX24, SDX55, SM8150, SXR1130 **CVE ID : CVE-2020-3651**	etins/april-2020-bulletin	
sm8150					
Reachable Assertion	16-04-2020	7.8	Active command timeout since WM status change cmd is not removed from active queue if peer sends multiple deauth frames. in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer	https://www.qualcomm.com/company/product-security/bulletins/april-2020-bulletin	H-QUA-SM81-010520/350

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables in APQ8009, APQ8017, APQ8053, APQ8096AU, MDM9206, MDM9207C, MDM9607, MDM9640, MDM9650, MSM8905, MSM8909W, MSM8917, MSM8920, MSM8937, MSM8940, MSM8953, MSM8996AU, QCA6174A, QCA6574AU, QCA9377, QCA9379, QCM2150, QCN7605, QCS605, QM215, SC8180X, SDM429, SDM429W, SDM439, SDM450, SDM630, SDM632, SDM636, SDM660, SDM845, SDX20, SDX24, SDX55, SM8150, SXR1130 **CVE ID : CVE-2020-3651**		
qm215					
Reachable Assertion	16-04-2020	7.8	Active command timeout since WM status change cmd is not removed from active queue if peer sends multiple deauth frames. in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon	https://www.qualcomm.com/company/product-security/bulletins/april-2020-bulletin	H-QUA-QM21-010520/351

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables in APQ8009, APQ8017, APQ8053, APQ8096AU, MDM9206, MDM9207C, MDM9607, MDM9640, MDM9650, MSM8905, MSM8909W, MSM8917, MSM8920, MSM8937, MSM8940, MSM8953, MSM8996AU, QCA6174A, QCA6574AU, QCA9377, QCA9379, QCM2150, QCN7605, QCS605, QM215, SC8180X, SDM429, SDM429W, SDM439, SDM450, SDM630, SDM632, SDM636, SDM660, SDM845, SDX20, SDX24, SDX55, SM8150, SXR1130 **CVE ID : CVE-2020-3651**		
sdm429					
Reachable Assertion	16-04-2020	7.8	Active command timeout since WM status change cmd is not removed from active queue if peer sends multiple deauth frames. in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice &	https://www.qualcomm.com/company/product-security/bulletins/april-2020-bulletin	H-QUA-SDM4-010520/352

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Music, Snapdragon Wearables in APQ8009, APQ8017, APQ8053, APQ8096AU, MDM9206, MDM9207C, MDM9607, MDM9640, MDM9650, MSM8905, MSM8909W, MSM8917, MSM8920, MSM8937, MSM8940, MSM8953, MSM8996AU, QCA6174A, QCA6574AU, QCA9377, QCA9379, QCM2150, QCN7605, QCS605, QM215, SC8180X, SDM429, SDM429W, SDM439, SDM450, SDM630, SDM632, SDM636, SDM660, SDM845, SDX20, SDX24, SDX55, SM8150, SXR1130 **CVE ID : CVE-2020-3651**		
sdm632					
Reachable Assertion	16-04-2020	7.8	Active command timeout since WM status change cmd is not removed from active queue if peer sends multiple deauth frames. in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables in APQ8009, APQ8017, APQ8053,	https://www.qualcomm.com/company/product-security/bulletins/april-2020-bulletin	H-QUA-SDM6-010520/353

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			APQ8096AU, MDM9206, MDM9207C, MDM9607, MDM9640, MDM9650, MSM8905, MSM8909W, MSM8917, MSM8920, MSM8937, MSM8940, MSM8953, MSM8996AU, QCA6174A, QCA6574AU, QCA9377, QCA9379, QCM2150, QCN7605, QCS605, QM215, SC8180X, SDM429, SDM429W, SDM439, SDM450, SDM630, SDM632, SDM636, SDM660, SDM845, SDX20, SDX24, SDX55, SM8150, SXR1130 **CVE ID : CVE-2020-3651**		
msm8917					
Reachable Assertion	16-04-2020	7.8	Active command timeout since WM status change cmd is not removed from active queue if peer sends multiple deauth frames. in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables in APQ8009, APQ8017, APQ8053, APQ8096AU, MDM9206, MDM9207C, MDM9607, MDM9640, MDM9650,	https://www.qualcomm.com/company/product-security/bulletins/april-2020-bulletin	H-QUA-MSM8-010520/354

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			MSM8905, MSM8909W, MSM8917, MSM8920, MSM8937, MSM8940, MSM8953, MSM8996AU, QCA6174A, QCA6574AU, QCA9377, QCA9379, QCM2150, QCN7605, QCS605, QM215, SC8180X, SDM429, SDM429W, SDM439, SDM450, SDM630, SDM632, SDM636, SDM660, SDM845, SDX20, SDX24, SDX55, SM8150, SXR1130 **CVE ID : CVE-2020-3651**		
msm8920					
Reachable Assertion	16-04-2020	7.8	Active command timeout since WM status change cmd is not removed from active queue if peer sends multiple deauth frames. in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables in APQ8009, APQ8017, APQ8053, APQ8096AU, MDM9206, MDM9207C, MDM9607, MDM9640, MDM9650, MSM8905, MSM8909W, MSM8917, MSM8920, MSM8937, MSM8940,	https://www.qualcomm.com/company/product-security/bulletins/april-2020-bulletin	H-QUA-MSM8-010520/355

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			MSM8953, MSM8996AU, QCA6174A, QCA6574AU, QCA9377, QCA9379, QCM2150, QCN7605, QCS605, QM215, SC8180X, SDM429, SDM429W, SDM439, SDM450, SDM630, SDM632, SDM636, SDM660, SDM845, SDX20, SDX24, SDX55, SM8150, SXR1130 **CVE ID : CVE-2020-3651**		
msm8937					
Reachable Assertion	16-04-2020	7.8	Active command timeout since WM status change cmd is not removed from active queue if peer sends multiple deauth frames. in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables in APQ8009, APQ8017, APQ8053, APQ8096AU, MDM9206, MDM9207C, MDM9607, MDM9640, MDM9650, MSM8905, MSM8909W, MSM8917, MSM8920, MSM8937, MSM8940, MSM8953, MSM8996AU, QCA6174A, QCA6574AU, QCA9377, QCA9379,	https://www.qualcomm.com/company/product-security/bulletins/april-2020-bulletin	H-QUA-MSM8-010520/356

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			QCM2150, QCN7605, QCS605, QM215, SC8180X, SDM429, SDM429W, SDM439, SDM450, SDM630, SDM632, SDM636, SDM660, SDM845, SDX20, SDX24, SDX55, SM8150, SXR1130 **CVE ID : CVE-2020-3651**		
msm8940					
Reachable Assertion	16-04-2020	7.8	Active command timeout since WM status change cmd is not removed from active queue if peer sends multiple deauth frames. in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables in APQ8009, APQ8017, APQ8053, APQ8096AU, MDM9206, MDM9207C, MDM9607, MDM9640, MDM9650, MSM8905, MSM8909W, MSM8917, MSM8920, MSM8937, MSM8940, MSM8953, MSM8996AU, QCA6174A, QCA6574AU, QCA9377, QCA9379, QCM2150, QCN7605, QCS605, QM215, SC8180X, SDM429,	https://www.qualcomm.com/company/product-security/bulletins/april-2020-bulletin	H-QUA-MSM8-010520/357

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			SDM429W, SDM439, SDM450, SDM630, SDM632, SDM636, SDM660, SDM845, SDX20, SDX24, SDX55, SM8150, SXR1130 **CVE ID : CVE-2020-3651**		
sdm450					
Reachable Assertion	16-04-2020	7.8	Active command timeout since WM status change cmd is not removed from active queue if peer sends multiple deauth frames. in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables in APQ8009, APQ8017, APQ8053, APQ8096AU, MDM9206, MDM9207C, MDM9607, MDM9640, MDM9650, MSM8905, MSM8909W, MSM8917, MSM8920, MSM8937, MSM8940, MSM8953, MSM8996AU, QCA6174A, QCA6574AU, QCA9377, QCA9379, QCM2150, QCN7605, QCS605, QM215, SC8180X, SDM429, SDM429W, SDM439, SDM450, SDM630, SDM632, SDM636,	https://www.qualcomm.com/company/product-security/bulletins/april-2020-bulletin	H-QUA-SDM4-010520/358

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			SDM660, SDM845, SDX20, SDX24, SDX55, SM8150, SXR1130 **CVE ID : CVE-2020-3651**		
sc8180x					
Reachable Assertion	16-04-2020	7.8	Active command timeout since WM status change cmd is not removed from active queue if peer sends multiple deauth frames. in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables in APQ8009, APQ8017, APQ8053, APQ8096AU, MDM9206, MDM9207C, MDM9607, MDM9640, MDM9650, MSM8905, MSM8909W, MSM8917, MSM8920, MSM8937, MSM8940, MSM8953, MSM8996AU, QCA6174A, QCA6574AU, QCA9377, QCA9379, QCM2150, QCN7605, QCS605, QM215, SC8180X, SDM429, SDM429W, SDM439, SDM450, SDM630, SDM632, SDM636, SDM660, SDM845, SDX20, SDX24, SDX55, SM8150, SXR1130	https://www.qualcomm.com/company/product-security/bulletins/april-2020-bulletin	H-QUA-SC81-010520/359

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2020-3651		
Out-of-bounds Read	16-04-2020	9.4	Possible buffer over-read issue in windows x86 wlan driver function while processing beacon or request frame due to lack of check of length of variable received. in Snapdragon Compute, Snapdragon Connectivity in MSM8998, QCA6390, SC7180, SC8180X, SDM850 **CVE ID : CVE-2020-3652**	https://www.qualcomm.com/company/product-security/bulletins/april-2020-bulletin	H-QUA-SC81-010520/360
Out-of-bounds Read	16-04-2020	9.4	Possible buffer over-read in windows wlan driver function due to lack of check of length of variable received from userspace in Snapdragon Compute, Snapdragon Connectivity in MSM8998, QCA6390, SC7180, SC8180X, SDM850 **CVE ID : CVE-2020-3653**	https://www.qualcomm.com/company/product-security/bulletins/april-2020-bulletin	H-QUA-SC81-010520/361
sdm850					
Out-of-bounds Read	16-04-2020	9.4	Possible buffer over-read issue in windows x86 wlan driver function while processing beacon or request frame due to lack of check of length of variable received. in Snapdragon Compute, Snapdragon Connectivity in MSM8998, QCA6390, SC7180, SC8180X, SDM850 **CVE ID : CVE-2020-3652**	https://www.qualcomm.com/company/product-security/bulletins/april-2020-bulletin	H-QUA-SDM8-010520/362

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Out-of-bounds Read	16-04-2020	9.4	Possible buffer over-read in windows wlan driver function due to lack of check of length of variable received from userspace in Snapdragon Compute, Snapdragon Connectivity in MSM8998, QCA6390, SC7180, SC8180X, SDM850 **CVE ID : CVE-2020-3653**	https://www.qualcomm.com/company/product-security/bulletins/april-2020-bulletin	H-QUA-SDM8-010520/363
qcm2150					
Reachable Assertion	16-04-2020	7.8	Active command timeout since WM status change cmd is not removed from active queue if peer sends multiple deauth frames. in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables in APQ8009, APQ8017, APQ8053, APQ8096AU, MDM9206, MDM9207C, MDM9607, MDM9640, MDM9650, MSM8905, MSM8909W, MSM8917, MSM8920, MSM8937, MSM8940, MSM8953, MSM8996AU, QCA6174A, QCA6574AU, QCA9377, QCA9379, QCM2150, QCN7605, QCS605, QM215,	https://www.qualcomm.com/company/product-security/bulletins/april-2020-bulletin	H-QUA-QCM2-010520/364

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			SC8180X, SDM429, SDM429W, SDM439, SDM450, SDM630, SDM632, SDM636, SDM660, SDM845, SDX20, SDX24, SDX55, SM8150, SXR1130 **CVE ID : CVE-2020-3651**		
sdx55					
Reachable Assertion	16-04-2020	7.8	Active command timeout since WM status change cmd is not removed from active queue if peer sends multiple deauth frames. in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables in APQ8009, APQ8017, APQ8053, APQ8096AU, MDM9206, MDM9207C, MDM9607, MDM9640, MDM9650, MSM8905, MSM8909W, MSM8917, MSM8920, MSM8937, MSM8940, MSM8953, MSM8996AU, QCA6174A, QCA6574AU, QCA9377, QCA9379, QCM2150, QCN7605, QCS605, QM215, SC8180X, SDM429, SDM429W, SDM439, SDM450, SDM630,	https://www.qualcomm.com/company/product-security/bulletins/april-2020-bulletin	H-QUA-SDX5-010520/365

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			SDM632, SDM636, SDM660, SDM845, SDX20, SDX24, SDX55, SM8150, SXR1130 **CVE ID : CVE-2020-3651**		
qca6390					
Out-of-bounds Read	16-04-2020	9.4	Possible buffer over-read issue in windows x86 wlan driver function while processing beacon or request frame due to lack of check of length of variable received. in Snapdragon Compute, Snapdragon Connectivity in MSM8998, QCA6390, SC7180, SC8180X, SDM850 **CVE ID : CVE-2020-3652**	https://www.qualcomm.com/company/product-security/bulletins/april-2020-bulletin	H-QUA-QCA6-010520/366
Out-of-bounds Read	16-04-2020	9.4	Possible buffer over-read in windows wlan driver function due to lack of check of length of variable received from userspace in Snapdragon Compute, Snapdragon Connectivity in MSM8998, QCA6390, SC7180, SC8180X, SDM850 **CVE ID : CVE-2020-3653**	https://www.qualcomm.com/company/product-security/bulletins/april-2020-bulletin	H-QUA-QCA6-010520/367
se					
tricon_tcm_4351					
Uncontrolled Resource Consumption	16-04-2020	5	**VERSION NOT SUPPORTED WHEN ASSIGNED** A vulnerability could cause TCM modules to reset when under high network	N/A	H-SE-TRIC-010520/368

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			load in TCM v10.4.x and in system v10.3.x. This vulnerability was discovered and remediated in version v10.5.x on August 13, 2009. TCMs from v10.5.x and on will no longer exhibit this behavior. **CVE ID : CVE-2020-7486**		
tricon_tcm_4352					
Uncontrolled Resource Consumption	16-04-2020	5	**VERSION NOT SUPPORTED WHEN ASSIGNED** A vulnerability could cause TCM modules to reset when under high network load in TCM v10.4.x and in system v10.3.x. This vulnerability was discovered and remediated in version v10.5.x on August 13, 2009. TCMs from v10.5.x and on will no longer exhibit this behavior. **CVE ID : CVE-2020-7486**	N/A	H-SE-TRIC-010520/369
tricon_tcm_4351a					
Uncontrolled Resource Consumption	16-04-2020	5	**VERSION NOT SUPPORTED WHEN ASSIGNED** A vulnerability could cause TCM modules to reset when under high network load in TCM v10.4.x and in system v10.3.x. This vulnerability was discovered and remediated in version	N/A	H-SE-TRIC-010520/370

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			v10.5.x on August 13, 2009. TCMs from v10.5.x and on will no longer exhibit this behavior. **CVE ID : CVE-2020-7486**		
tricon_tcm_4351b					
Uncontrolled Resource Consumption	16-04-2020	5	**VERSION NOT SUPPORTED WHEN ASSIGNED** A vulnerability could cause TCM modules to reset when under high network load in TCM v10.4.x and in system v10.3.x. This vulnerability was discovered and remediated in version v10.5.x on August 13, 2009. TCMs from v10.5.x and on will no longer exhibit this behavior. **CVE ID : CVE-2020-7486**	N/A	H-SE-TRIC-010520/371
tricon_tcm_4352a					
Uncontrolled Resource Consumption	16-04-2020	5	**VERSION NOT SUPPORTED WHEN ASSIGNED** A vulnerability could cause TCM modules to reset when under high network load in TCM v10.4.x and in system v10.3.x. This vulnerability was discovered and remediated in version v10.5.x on August 13, 2009. TCMs from v10.5.x and on will no longer exhibit this behavior. **CVE ID : CVE-2020-7486**	N/A	H-SE-TRIC-010520/372

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
tricon_tcm_4352b					
Uncontrolled Resource Consumption	16-04-2020	5	**VERSION NOT SUPPORTED WHEN ASSIGNED** A vulnerability could cause TCM modules to reset when under high network load in TCM v10.4.x and in system v10.3.x. This vulnerability was discovered and remediated in version v10.5.x on August 13, 2009. TCMs from v10.5.x and on will no longer exhibit this behavior. **CVE ID : CVE-2020-7486**	N/A	H-SE-TRIC-010520/373
modicon_m218					
Insufficient Verification of Data Authenticity	22-04-2020	7.5	A CWE-345: Insufficient Verification of Data Authenticity vulnerability exists which could allow the attacker to execute malicious code on the Modicon M218, M241, M251, and M258 controllers. **CVE ID : CVE-2020-7487**	N/A	H-SE-MODI-010520/374
Cleartext Transmission of Sensitive Information	22-04-2020	5	A CWE-319: Cleartext Transmission of Sensitive Information vulnerability exists which could leak sensitive information transmitted between the software and the Modicon M218, M241, M251, and M258 controllers. **CVE ID : CVE-2020-7488**	N/A	H-SE-MODI-010520/375

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
modicon_m241					
Insufficient Verification of Data Authenticity	22-04-2020	7.5	A CWE-345: Insufficient Verification of Data Authenticity vulnerability exists which could allow the attacker to execute malicious code on the Modicon M218, M241, M251, and M258 controllers. **CVE ID : CVE-2020-7487**	N/A	H-SE-MODI-010520/376
Cleartext Transmission of Sensitive Information	22-04-2020	5	A CWE-319: Cleartext Transmission of Sensitive Information vulnerability exists which could leak sensitive information transmitted between the software and the Modicon M218, M241, M251, and M258 controllers. **CVE ID : CVE-2020-7488**	N/A	H-SE-MODI-010520/377
modicon_m251					
Insufficient Verification of Data Authenticity	22-04-2020	7.5	A CWE-345: Insufficient Verification of Data Authenticity vulnerability exists which could allow the attacker to execute malicious code on the Modicon M218, M241, M251, and M258 controllers. **CVE ID : CVE-2020-7487**	N/A	H-SE-MODI-010520/378
Cleartext Transmission of Sensitive Information	22-04-2020	5	A CWE-319: Cleartext Transmission of Sensitive Information vulnerability exists which could leak sensitive information transmitted between the software and the Modicon	N/A	H-SE-MODI-010520/379

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			M218, M241, M251, and M258 controllers. **CVE ID : CVE-2020-7488**		
modicon_m258					
Insufficient Verification of Data Authenticity	22-04-2020	7.5	A CWE-345: Insufficient Verification of Data Authenticity vulnerability exists which could allow the attacker to execute malicious code on the Modicon M218, M241, M251, and M258 controllers. **CVE ID : CVE-2020-7487**	N/A	H-SE-MODI-010520/380
Cleartext Transmission of Sensitive Information	22-04-2020	5	A CWE-319: Cleartext Transmission of Sensitive Information vulnerability exists which could leak sensitive information transmitted between the software and the Modicon M218, M241, M251, and M258 controllers. **CVE ID : CVE-2020-7488**	N/A	H-SE-MODI-010520/381