Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Application					
360totalsecurity					
360_total_security					
Untrusted Search Path	21-Jul-20	6.9	In version 12.1.0.1004 and below of 360 Total Security,when TPI calls the browser process, there exists a local privilege escalation vulnerability. An attacker who could exploit DLL hijacking could execute arbitrary code on the Local system. **CVE ID : CVE-2020-15722**	N/A	A-360-360_-190820/1
Untrusted Search Path	21-Jul-20	6.9	In the version 12.1.0.1004 and below of 360 Total Security, when the main process of 360 Total Security calls GameChrome.exe, there exists a local privilege escalation vulnerability. An attacker who could exploit DLL hijacking to bypass the hips could execute arbitrary code on the Local system. **CVE ID : CVE-2020-15723**	N/A	A-360-360_-190820/2
Untrusted Search Path	21-Jul-20	6.9	In the version 12.1.0.1005 and below of 360 Total Security, when the Gamefolde calls GameChrome.exe, there exists a local privilege	N/A	A-360-360_-190820/3

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			escalation vulnerability. An attacker who could exploit DLL hijacking to bypass the hips could execute arbitrary code on the Local system. **CVE ID : CVE-2020-15724**		
Adobe					
download_manager					
Improper Neutralization of Special Elements in Output Used by a Downstream Component ('Injection')	17-Jul-20	9.3	Adobe Download Manager version 2.0.0.518 have a command injection vulnerability. Successful exploitation could lead to arbitrary code execution. **CVE ID : CVE-2020-9688**	https://helpx.adobe.com/security/products/adm/apsb20-49.html	A-ADO-DOWN-190820/4
coldfusion					
Untrusted Search Path	17-Jul-20	4.4	Adobe ColdFusion 2016 update 15 and earlier versions, and ColdFusion 2018 update 9 and earlier versions have a dll search-order hijacking vulnerability. Successful exploitation could lead to privilege escalation. **CVE ID : CVE-2020-9672**	https://helpx.adobe.com/security/products/coldfusion/apsb20-43.html	A-ADO-COLD-190820/5
Untrusted Search Path	17-Jul-20	4.4	Adobe ColdFusion 2016 update 15 and earlier versions, and ColdFusion 2018 update 9 and earlier versions have a dll search-order hijacking vulnerability. Successful exploitation could lead to privilege escalation.	https://helpx.adobe.com/security/products/coldfusion/apsb20-43.html	A-ADO-COLD-190820/6

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2020-9673		
creative_cloud					
Improper Privilege Management	17-Jul-20	7.5	Adobe Creative Cloud Desktop Application versions 5.1 and earlier have a lack of exploit mitigations vulnerability. Successful exploitation could lead to privilege escalation. **CVE ID : CVE-2020-9669**	https://helpx.adobe.com/security/products/creative-cloud/apsb20-33.html	A-ADO-CREA-190820/7
adobe_reader					
Improper Limitation of a Pathname to a Restricted Directory ('Path Traversal')	22-Jul-20	5	Adobe Reader Mobile versions 20.0.1 and earlier have a directory traversal vulnerability. Successful exploitation could lead to information disclosure. **CVE ID : CVE-2020-9663**	https://helpx.adobe.com/security/products/reader-mobile/apsb20-50.html	A-ADO-ADOB-190820/8
creative_cloud_desktop_application					
Improper Link Resolution Before File Access ('Link Following')	17-Jul-20	7.5	Adobe Creative Cloud Desktop Application versions 5.1 and earlier have a symlink vulnerability vulnerability. Successful exploitation could lead to privilege escalation. **CVE ID : CVE-2020-9670**	https://helpx.adobe.com/security/products/creative-cloud/apsb20-33.html	A-ADO-CREA-190820/9
creative_cloud_desktop_applocation					
Improper Privilege Management	17-Jul-20	7.5	Adobe Creative Cloud Desktop Application versions 5.1 and earlier have an insecure file permissions vulnerability. Successful exploitation could lead to privilege	https://helpx.adobe.com/security/products/creative-cloud/apsb20-33.html	A-ADO-CREA-190820/10

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			escalation. **CVE ID : CVE-2020-9671**		
Improper Link Resolution Before File Access ('Link Following')	17-Jul-20	10	Adobe Creative Cloud Desktop Application versions 5.1 and earlier have a symlink vulnerability vulnerability. Successful exploitation could lead to arbitrary file system write. **CVE ID : CVE-2020-9682**	https://helpx.adobe.com/security/products/creative-cloud/apsb20-33.html	A-ADO-CREA-190820/11
prelude					
Out-of-bounds Write	22-Jul-20	6.8	Adobe Prelude versions 9.0 and earlier have an out-of-bounds read vulnerability. Successful exploitation could lead to arbitrary code execution. **CVE ID : CVE-2020-9677**	https://helpx.adobe.com/security/products/prelude/apsb20-46.html	A-ADO-PREL-190820/12
Out-of-bounds Write	22-Jul-20	6.8	Adobe Prelude versions 9.0 and earlier have an out-of-bounds write vulnerability. Successful exploitation could lead to arbitrary code execution . **CVE ID : CVE-2020-9678**	https://helpx.adobe.com/security/products/prelude/apsb20-46.html	A-ADO-PREL-190820/13
Out-of-bounds Read	22-Jul-20	4.3	Adobe Prelude versions 9.0 and earlier have an out-of-bounds read vulnerability. Successful exploitation could lead to arbitrary code execution. **CVE ID : CVE-2020-9679**	https://helpx.adobe.com/security/products/prelude/apsb20-46.html	A-ADO-PREL-190820/14
Out-of-bounds Write	22-Jul-20	6.8	Adobe Prelude versions 9.0 and earlier have an out-of-bounds write vulnerability. Successful exploitation could lead to	https://helpx.adobe.com/security/products/prelude/apsb20-	A-ADO-PREL-190820/15

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			arbitrary code execution . **CVE ID : CVE-2020-9680**	46.html	
photoshop					
Out-of-bounds Write	22-Jul-20	6.8	Adobe Photoshop versions Photoshop CC 2019, and Photoshop 2020 have an out-of-bounds read vulnerability. Successful exploitation could lead to arbitrary code execution. **CVE ID : CVE-2020-9683**	https://helpx.adobe.com/security/products/photoshop/apsb20-45.html	A-ADO-PHOT-190820/16
Out-of-bounds Write	22-Jul-20	6.8	Adobe Photoshop versions Photoshop CC 2019, and Photoshop 2020 have an out-of-bounds write vulnerability. Successful exploitation could lead to arbitrary code execution . **CVE ID : CVE-2020-9684**	https://helpx.adobe.com/security/products/photoshop/apsb20-45.html	A-ADO-PHOT-190820/17
Out-of-bounds Write	22-Jul-20	6.8	Adobe Photoshop versions Photoshop CC 2019, and Photoshop 2020 have an out-of-bounds write vulnerability. Successful exploitation could lead to arbitrary code execution . **CVE ID : CVE-2020-9685**	https://helpx.adobe.com/security/products/photoshop/apsb20-45.html	A-ADO-PHOT-190820/18
Out-of-bounds Read	22-Jul-20	4.3	Adobe Photoshop versions Photoshop CC 2019, and Photoshop 2020 have an out-of-bounds read vulnerability. Successful exploitation could lead to arbitrary code execution. **CVE ID : CVE-2020-9686**	https://helpx.adobe.com/security/products/photoshop/apsb20-45.html	A-ADO-PHOT-190820/19
Out-of-bounds	22-Jul-20	6.8	Adobe Photoshop versions Photoshop CC 2019, and Photoshop 2020 have an	https://helpx.adobe.com/security/pr	A-ADO-PHOT-190820/20

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Write			out-of-bounds write vulnerability. Successful exploitation could lead to arbitrary code execution . **CVE ID : CVE-2020-9687**	oducts/photoshop/apsb20-45.html	
media_encoder					
Out-of-bounds Write	17-Jul-20	6.8	Adobe Media Encoder versions 14.2 and earlier have an out-of-bounds write vulnerability. Successful exploitation could lead to arbitrary code execution. **CVE ID : CVE-2020-9646**	https://helpx.adobe.com/security/products/media-encoder/apsb20-36.html	A-ADO-MEDI-190820/21
Out-of-bounds Read	17-Jul-20	4.3	Adobe Media Encoder versions 14.2 and earlier have an out-of-bounds read vulnerability. Successful exploitation could lead to information disclosure. **CVE ID : CVE-2020-9649**	https://helpx.adobe.com/security/products/media-encoder/apsb20-36.html	A-ADO-MEDI-190820/22
Out-of-bounds Write	17-Jul-20	6.8	Adobe Media Encoder versions 14.2 and earlier have an out-of-bounds write vulnerability. Successful exploitation could lead to arbitrary code execution. **CVE ID : CVE-2020-9650**	https://helpx.adobe.com/security/products/media-encoder/apsb20-36.html	A-ADO-MEDI-190820/23
photoshop_cc					
Out-of-bounds Write	22-Jul-20	6.8	Adobe Photoshop versions Photoshop CC 2019, and Photoshop 2020 have an out-of-bounds read vulnerability. Successful exploitation could lead to arbitrary code execution.	https://helpx.adobe.com/security/products/photoshop/apsb20-45.html	A-ADO-PHOT-190820/24

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2020-9683		
Out-of-bounds Write	22-Jul-20	6.8	Adobe Photoshop versions Photoshop CC 2019, and Photoshop 2020 have an out-of-bounds write vulnerability. Successful exploitation could lead to arbitrary code execution . **CVE ID : CVE-2020-9684**	https://helpx.adobe.com/security/products/photoshop/apsb20-45.html	A-ADO-PHOT-190820/25
Out-of-bounds Write	22-Jul-20	6.8	Adobe Photoshop versions Photoshop CC 2019, and Photoshop 2020 have an out-of-bounds write vulnerability. Successful exploitation could lead to arbitrary code execution . **CVE ID : CVE-2020-9685**	https://helpx.adobe.com/security/products/photoshop/apsb20-45.html	A-ADO-PHOT-190820/26
Out-of-bounds Read	22-Jul-20	4.3	Adobe Photoshop versions Photoshop CC 2019, and Photoshop 2020 have an out-of-bounds read vulnerability. Successful exploitation could lead to arbitrary code execution. **CVE ID : CVE-2020-9686**	https://helpx.adobe.com/security/products/photoshop/apsb20-45.html	A-ADO-PHOT-190820/27
Out-of-bounds Write	22-Jul-20	6.8	Adobe Photoshop versions Photoshop CC 2019, and Photoshop 2020 have an out-of-bounds write vulnerability. Successful exploitation could lead to arbitrary code execution . **CVE ID : CVE-2020-9687**	https://helpx.adobe.com/security/products/photoshop/apsb20-45.html	A-ADO-PHOT-190820/28
bridge					
Out-of-bounds Write	22-Jul-20	6.8	Adobe Bridge versions 10.0.3 and earlier have an out-of-bounds write vulnerability. Successful	https://helpx.adobe.com/security/products/bridg	A-ADO-BRID-190820/29

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			exploitation could lead to arbitrary code execution. **CVE ID : CVE-2020-9674**	e/apsb20-44.html	
Out-of-bounds Read	22-Jul-20	6.8	Adobe Bridge versions 10.0.3 and earlier have an out-of-bounds read vulnerability. Successful exploitation could lead to arbitrary code execution. **CVE ID : CVE-2020-9675**	https://helpx.adobe.com/security/products/bridge/apsb20-44.html	A-ADO-BRID-190820/30
Out-of-bounds Write	22-Jul-20	6.8	Adobe Bridge versions 10.0.3 and earlier have an out-of-bounds write vulnerability. Successful exploitation could lead to arbitrary code execution. **CVE ID : CVE-2020-9676**	https://helpx.adobe.com/security/products/bridge/apsb20-44.html	A-ADO-BRID-190820/31
AMD					
radeon_directx_11_driver_atidxx64.dll					
Out-of-bounds Write	20-Jul-20	6.5	An exploitable memory corruption vulnerability exists in AMD atidxx64.dll 26.20.15019.19000 graphics driver. A specially crafted pixel shader can cause memory corruption vulnerability. An attacker can provide a specially crafted shader file to trigger this vulnerability. This vulnerability potentially could be triggered from guest machines running virtualization environments (ie. VMware, qemu, VirtualBox etc.) in order to perform guest-to-host escape - as it was	N/A	A-AMD-RADE-190820/32

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			demonstrated before (TALOS-2018-0533, TALOS-2018-0568, etc.). Theoretically this vulnerability could be also triggered from web browser (using webGL and webassembly). This vulnerability was triggered from HYPER-V guest using RemoteFX feature leading to executing the vulnerable code on the HYPER-V host (inside of the rdvgm.exe process). **CVE ID : CVE-2020-6100**		
Out-of-bounds Write	20-Jul-20	6.5	An exploitable code execution vulnerability exists in the Shader functionality of AMD Radeon DirectX 11 Driver atidxx64.dll 26.20.15019.19000. An attacker can provide a specially crafted shader file to trigger this vulnerability, resulting in code execution. This vulnerability can be triggered from a HYPER-V guest using the RemoteFX feature, leading to executing the vulnerable code on the HYPER-V host (inside of the rdvgm.exe process). Theoretically this vulnerability could be also triggered from web browser (using webGL and webassembly).	N/A	A-AMD-RADE-190820/33

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2020-6101		
Improper Input Validation	20-Jul-20	6.5	An exploitable code execution vulnerability exists in the Shader functionality of AMD Radeon DirectX 11 Driver atidxx64.dll 26.20.15019.19000. An attacker can provide a a specially crafted shader file to trigger this vulnerability, resulting in code execution. This vulnerability can be triggered from a HYPER-V guest using the RemoteFX feature, leading to executing the vulnerable code on the HYPER-V host (inside of the rdvgm.exe process). Theoretically this vulnerability could be also triggered from web browser (using webGL and webassembly). **CVE ID : CVE-2020-6102**	N/A	A-AMD-RADE-190820/34
Out-of-bounds Write	20-Jul-20	6.5	An exploitable code execution vulnerability exists in the Shader functionality of AMD Radeon DirectX 11 Driver atidxx64.dll 26.20.15019.19000. An attacker can provide a a specially crafted shader file to trigger this vulnerability, resulting in code execution. This vulnerability can be triggered from a HYPER-V	N/A	A-AMD-RADE-190820/35

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			guest using the RemoteFX feature, leading to executing the vulnerable code on the HYPER-V host (inside of the rdvgm.exe process). Theoretically this vulnerability could be also triggered from web browser (using webGL and webassembly). **CVE ID : CVE-2020-6103**		
Apache					
airflow					
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	17-Jul-20	4.3	An issue was found in Apache Airflow versions 1.10.10 and below. A stored XSS vulnerability was discovered in the Chart pages of the the "classic" UI. **CVE ID : CVE-2020-9485**	N/A	A-APA-AIRF-190820/36
Improper Neutralization of Special Elements used in an OS Command ('OS Command Injection')	17-Jul-20	6.5	An issue was found in Apache Airflow versions 1.10.10 and below. A remote code/command injection vulnerability was discovered in one of the example DAGs shipped with Airflow which would allow any authenticated user to run arbitrary commands as the user running airflow worker/scheduler (depending on the executor in use). If you already have examples disabled by setting load_examples=False in	N/A	A-APA-AIRF-190820/37

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			the config then you are not vulnerable. **CVE ID : CVE-2020-11978**		
Improper Neutralization of Special Elements used in an OS Command ('OS Command Injection')	17-Jul-20	7.5	An issue was found in Apache Airflow versions 1.10.10 and below. When using CeleryExecutor, if an attacker can connect to the broker (Redis, RabbitMQ) directly, it is possible to inject commands, resulting in the celery worker running arbitrary commands. **CVE ID : CVE-2020-11981**	N/A	A-APA-AIRF-190820/38
Deserialization of Untrusted Data	17-Jul-20	7.5	An issue was found in Apache Airflow versions 1.10.10 and below. When using CeleryExecutor, if an attack can connect to the broker (Redis, RabbitMQ) directly, it was possible to insert a malicious payload directly to the broker which could lead to a deserialization attack (and thus remote code execution) on the Worker. **CVE ID : CVE-2020-11982**	N/A	A-APA-AIRF-190820/39
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	17-Jul-20	3.5	An issue was found in Apache Airflow versions 1.10.10 and below. It was discovered that many of the admin management screens in the new/RBAC UI handled escaping incorrectly, allowing authenticated users with appropriate permissions	N/A	A-APA-AIRF-190820/40

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			to create stored XSS attacks. **CVE ID : CVE-2020-11983**		
activemq_artemis					
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	20-Jul-20	4.3	In Apache ActiveMQ Artemis 2.5.0 to 2.13.0, a specially crafted MQTT packet which has an XSS payload as client-id or topic name can exploit this vulnerability. The XSS payload is being injected into the admin console's browser. The XSS payload is triggered in the diagram plugin; queue node and the info section. **CVE ID : CVE-2020-13932**	N/A	A-APA-ACTI-190820/41
articatech					
artica_proxy					
Improper Neutralization of Special Elements used in an SQL Command ('SQL Injection')	20-Jul-20	5	An issue was discovered in Artica Proxy CE before 4.28.030.418. SQL Injection exists via the Netmask, Hostname, and Alias fields. **CVE ID : CVE-2020-15052**	N/A	A-ART-ARTI-190820/42
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	20-Jul-20	4.3	An issue was discovered in Artica Proxy CE before 4.28.030.418. Reflected XSS exists via these search fields: real time request, System Events, Proxy Events, Proxy Objects, and Firewall objects. **CVE ID : CVE-2020-15053**	N/A	A-ART-ARTI-190820/43

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Artifex					
ghostscript					
Improper Restriction of Operations within the Bounds of a Memory Buffer	28-Jul-20	7.5	A memory corruption issue was found in Artifex Ghostscript 9.50 and 9.52. Use of a non-standard PostScript operator can allow overriding of file access controls. The 'rsearch' calculation for the 'post' size resulted in a size that was too large, and could underflow to max uint32_t. This was fixed in commit 5d499272b95a6b890a1397e11d20937de000d31b. **CVE ID : CVE-2020-15900**	https://artifex.com/security-advisories/CVE-2020-15900	A-ART-GHOS-190820/44
Asus					
screenpad2_upgrade_tool					
Untrusted Search Path	20-Jul-20	4.4	AsusScreenXpertServicec.exe and ScreenXpertUpgradeServiceManager.exe in ScreenPad2_Upgrade_Tool.msi V1.0.3 for ASUS PCs with ScreenPad 1.0 (UX450FDX, UX550GDX and UX550GEX) could lead to unsigned code execution with no additional restrictions when a user puts an application at a particular path with a particular file name. **CVE ID : CVE-2020-15009**	https://www.asus.com/Static_WebPage/ASUS-Product-Security-Advisory/, https://www.asus.com/support/FAQ/1043674	A-ASU-SCRE-190820/45
Atlassian					

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
data_center					
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	24-Jul-20	3.5	Affected versions of Atlassian Confluence Server and Data Center allow remote attackers to inject arbitrary HTML or JavaScript via a Cross-Site Scripting (XSS) vulnerability in user macro parameters. The affected versions are before version 7.4.2, and from version 7.5.0 before 7.5.2. **CVE ID : CVE-2020-14175**	N/A	A-ATL-DATA-190820/46
confluence					
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	24-Jul-20	3.5	Affected versions of Atlassian Confluence Server and Data Center allow remote attackers to inject arbitrary HTML or JavaScript via a Cross-Site Scripting (XSS) vulnerability in user macro parameters. The affected versions are before version 7.4.2, and from version 7.5.0 before 7.5.2. **CVE ID : CVE-2020-14175**	N/A	A-ATL-CONF-190820/47
auth0					
auth0					
Information Exposure Through an Error Message	29-Jul-20	4	In auth0 (npm package) versions before 2.27.1, a DenyList of specific keys that should be sanitized from the request object contained in the error object is used. The key for Authorization header is not sanitized and in	https://github.com/auth0/node-auth0/security/advisories/GHSA-5jpf-pj32-xx53	A-AUT-AUTH-190820/48

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			certain cases the Authorization header value can be logged exposing a bearer token. You are affected by this vulnerability if you are using the auth0 npm package, and you are using a Machine to Machine application authorized to use Auth0's management API **CVE ID : CVE-2020-15125**		
Automattic					
canvas					
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	20-Jul-20	6.8	A buffer overflow is present in canvas version <= 1.6.9, which could lead to a Denial of Service or execution of arbitrary code when it processes a user-provided image. **CVE ID : CVE-2020-8215**	N/A	A-AUT-CANV-190820/49
bitwarden					
server					
Server-Side Request Forgery (SSRF)	21-Jul-20	5	Bitwarden Server 1.35.1 allows SSRF because it does not consider certain IPv6 addresses (ones beginning with fc, fd, fe, or ff, and the :: address) and certain IPv4 addresses (0.0.0.0/8, 127.0.0.0/8, and 169.254.0.0/16). **CVE ID : CVE-2020-15879**	N/A	A-BIT-SERV-190820/50
cauldrondevelopment					
c\!					

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Improper Limitation of a Pathname to a Restricted Directory ('Path Traversal')	23-Jul-20	5	tar/TarFileReader.cpp in Cauldron cbang (aka C-Bang or C!) before 1.6.0 allows Directory Traversal during extraction from a TAR archive. **CVE ID : CVE-2020-15908**	N/A	A-CAU-C\!-190820/51
centos-webpanel					
centos_web_panel					
Improper Neutralization of Special Elements used in an OS Command ('OS Command Injection')	28-Jul-20	10	This vulnerability allows remote attackers to execute arbitrary code on affected installations of CentOS Web Panel cwp-el7-0.9.8.891. Authentication is not required to exploit this vulnerability. The specific flaw exists within loader_ajax.php. When parsing the line parameter, the process does not properly validate a user-supplied string before using it to execute a system call. An attacker can leverage this vulnerability to execute code in the context of root. Was ZDI-CAN-9259. **CVE ID : CVE-2020-15420**	N/A	A-CEN-CENT-190820/52
Improper Neutralization of Special Elements used in an OS Command ('OS Command	28-Jul-20	10	This vulnerability allows remote attackers to execute arbitrary code on affected installations of CentOS Web Panel cwp-e17.0.9.8.923. Authentication is not required to exploit this	N/A	A-CEN-CENT-190820/53

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Injection')			vulnerability. The specific flaw exists within ajax_mod_security.php. When parsing the check_ip parameter, the process does not properly validate a user-supplied string before using it to execute a system call. An attacker can leverage this vulnerability to execute code in the context of root. Was ZDI-CAN-9707. **CVE ID : CVE-2020-15421**		
Improper Neutralization of Special Elements used in an OS Command ('OS Command Injection')	28-Jul-20	10	This vulnerability allows remote attackers to execute arbitrary code on affected installations of CentOS Web Panel cwp-e17.0.9.8.923. Authentication is not required to exploit this vulnerability. The specific flaw exists within ajax_mod_security.php. When parsing the archivo parameter, the process does not properly validate a user-supplied string before using it to execute a system call. An attacker can leverage this vulnerability to execute code in the context of root. Was ZDI-CAN-9731. **CVE ID : CVE-2020-15422**	N/A	A-CEN-CENT-190820/54
Improper Neutralization of Special Elements	28-Jul-20	10	This vulnerability allows remote attackers to execute arbitrary code on affected installations of	N/A	A-CEN-CENT-190820/55

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
used in an OS Command ('OS Command Injection')			CentOS Web Panel cwp-e17.0.9.8.923. Authentication is not required to exploit this vulnerability. The specific flaw exists within ajax_mod_security.php. When parsing the dominio parameter, the process does not properly validate a user-supplied string before using it to execute a system call. An attacker can leverage this vulnerability to execute code in the context of root. Was ZDI-CAN-9732. **CVE ID : CVE-2020-15423**		
Improper Neutralization of Special Elements used in an OS Command ('OS Command Injection')	28-Jul-20	10	This vulnerability allows remote attackers to execute arbitrary code on affected installations of CentOS Web Panel cwp-e17.0.9.8.923. Authentication is not required to exploit this vulnerability. The specific flaw exists within ajax_mod_security.php. When parsing the domain parameter, the process does not properly validate a user-supplied string before using it to execute a system call. An attacker can leverage this vulnerability to execute code in the context of root. Was ZDI-CAN-9735. **CVE ID : CVE-2020-15424**	N/A	A-CEN-CENT-190820/56

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Improper Neutralization of Special Elements used in an OS Command ('OS Command Injection')	28-Jul-20	10	This vulnerability allows remote attackers to execute arbitrary code on affected installations of CentOS Web Panel cwp-e17.0.9.8.923. Authentication is not required to exploit this vulnerability. The specific flaw exists within ajax_mod_security.php. The issue results from the lack of proper validation of a user-supplied string before using it to execute a system call. An attacker can leverage this vulnerability to execute code in the context of root. Was ZDI-CAN-9742. **CVE ID : CVE-2020-15425**	N/A	A-CEN-CENT-190820/57
Improper Neutralization of Special Elements used in an OS Command ('OS Command Injection')	28-Jul-20	10	This vulnerability allows remote attackers to execute arbitrary code on affected installations of CentOS Web Panel cwp-e17.0.9.8.923. Authentication is not required to exploit this vulnerability. The specific flaw exists within ajax_migration_cpanel.php. When parsing the serverip parameter, the process does not properly validate a user-supplied string before using it to execute a system call. An attacker can leverage this vulnerability to execute code in the context of root.	N/A	A-CEN-CENT-190820/58

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Was ZDI-CAN-9709. **CVE ID : CVE-2020-15426**		
Improper Neutralization of Special Elements used in an OS Command ('OS Command Injection')	28-Jul-20	10	This vulnerability allows remote attackers to execute arbitrary code on affected installations of CentOS Web Panel cwp-e17.0.9.8.923. Authentication is not required to exploit this vulnerability. The specific flaw exists within ajax_disk_usage.php. When parsing the folderName parameter, the process does not properly validate a user-supplied string before using it to execute a system call. An attacker can leverage this vulnerability to execute code in the context of root. Was ZDI-CAN-9713. **CVE ID : CVE-2020-15427**	N/A	A-CEN-CENT-190820/59
Improper Neutralization of Special Elements used in an OS Command ('OS Command Injection')	28-Jul-20	10	This vulnerability allows remote attackers to execute arbitrary code on affected installations of CentOS Web Panel cwp-e17.0.9.8.923. Authentication is not required to exploit this vulnerability. The specific flaw exists within ajax_crons.php. When parsing the line parameter, the process does not properly validate a user-supplied string before using it to execute a	N/A	A-CEN-CENT-190820/60

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			system call. An attacker can leverage this vulnerability to execute code in the context of root. Was ZDI-CAN-9714. **CVE ID : CVE-2020-15428**		
Improper Neutralization of Special Elements used in an OS Command ('OS Command Injection')	28-Jul-20	10	This vulnerability allows remote attackers to execute arbitrary code on affected installations of CentOS Web Panel cwp-e17.0.9.8.923. Authentication is not required to exploit this vulnerability. The specific flaw exists within ajax_crons.php. When parsing the user parameter, the process does not properly validate a user-supplied string before using it to execute a system call. An attacker can leverage this vulnerability to execute code in the context of root. Was ZDI-CAN-9716. **CVE ID : CVE-2020-15429**	N/A	A-CEN-CENT-190820/61
Improper Neutralization of Special Elements used in an OS Command ('OS Command Injection')	28-Jul-20	10	This vulnerability allows remote attackers to execute arbitrary code on affected installations of CentOS Web Panel cwp-e17.0.9.8.923. Authentication is not required to exploit this vulnerability. The specific flaw exists within ajax_list_accounts.php. When parsing the	N/A	A-CEN-CENT-190820/62

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			username parameter, the process does not properly validate a user-supplied string before using it to execute a system call. An attacker can leverage this vulnerability to execute code in the context of root. Was ZDI-CAN-9736. **CVE ID : CVE-2020-15430**		
Improper Neutralization of Special Elements used in an OS Command ('OS Command Injection')	28-Jul-20	10	This vulnerability allows remote attackers to execute arbitrary code on affected installations of CentOS Web Panel cwp-e17.0.9.8.923. Authentication is not required to exploit this vulnerability. The specific flaw exists within ajax_crons.php. When parsing the user parameter, the process does not properly validate a user-supplied string before using it to execute a system call. An attacker can leverage this vulnerability to execute code in the context of root. Was ZDI-CAN-9740. **CVE ID : CVE-2020-15431**	N/A	A-CEN-CENT-190820/63
Improper Neutralization of Special Elements used in an OS Command ('OS Command	28-Jul-20	10	This vulnerability allows remote attackers to execute arbitrary code on affected installations of CentOS Web Panel cwp-e17.0.9.8.923. Authentication is not required to exploit this	N/A	A-CEN-CENT-190820/64

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Injection')			vulnerability. The specific flaw exists within ajax_migration_cpanel.php. When parsing the filespace parameter, the process does not properly validate a user-supplied string before using it to execute a system call. An attacker can leverage this vulnerability to execute code in the context of root. Was ZDI-CAN-9743. **CVE ID : CVE-2020-15432**		
Improper Neutralization of Special Elements used in an OS Command ('OS Command Injection')	28-Jul-20	10	This vulnerability allows remote attackers to execute arbitrary code on affected installations of CentOS Web Panel cwp-e17.0.9.8.923. Authentication is not required to exploit this vulnerability. The specific flaw exists within ajax_php_pecl.php. When parsing the phpversion parameter, the process does not properly validate a user-supplied string before using it to execute a system call. An attacker can leverage this vulnerability to execute code in the context of root. Was ZDI-CAN-9715. **CVE ID : CVE-2020-15433**	N/A	A-CEN-CENT-190820/65
Improper Neutralization of Special Elements	28-Jul-20	10	This vulnerability allows remote attackers to execute arbitrary code on affected installations of	N/A	A-CEN-CENT-190820/66

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
used in an OS Command ('OS Command Injection')			CentOS Web Panel cwp-e17.0.9.8.923. Authentication is not required to exploit this vulnerability. The specific flaw exists within ajax_php_pecl.php. When parsing the canal parameter, the process does not properly validate a user-supplied string before using it to execute a system call. An attacker can leverage this vulnerability to execute code in the context of root. Was ZDI-CAN-9745. **CVE ID : CVE-2020-15434**		
Improper Neutralization of Special Elements used in an OS Command ('OS Command Injection')	28-Jul-20	10	This vulnerability allows remote attackers to execute arbitrary code on affected installations of CentOS Web Panel cwp-e17.0.9.8.923. Authentication is not required to exploit this vulnerability. The specific flaw exists within ajax_dashboard.php. When parsing the service_start parameter, the process does not properly validate a user-supplied string before using it to execute a system call. An attacker can leverage this vulnerability to execute code in the context of root. Was ZDI-CAN-9719. **CVE ID : CVE-2020-15435**	N/A	A-CEN-CENT-190820/67

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Improper Neutralization of Special Elements used in an OS Command ('OS Command Injection')	28-Jul-20	10	This vulnerability allows remote attackers to execute arbitrary code on affected installations of CentOS Web Panel cwp-e17.0.9.8.923. Authentication is not required to exploit this vulnerability. The specific flaw exists within ajax_admin_apis.php. The issue results from the lack of proper validation of a user-supplied string before using it to execute a system call. An attacker can leverage this vulnerability to execute code in the context of root. Was ZDI-CAN-9720. **CVE ID : CVE-2020-15606**	N/A	A-CEN-CENT-190820/68
Improper Neutralization of Special Elements used in an OS Command ('OS Command Injection')	28-Jul-20	10	This vulnerability allows remote attackers to execute arbitrary code on affected installations of CentOS Web Panel cwp-e17.0.9.8.923. Authentication is not required to exploit this vulnerability. The specific flaw exists within ajax_admin_apis.php. When parsing the line parameter, the process does not properly validate a user-supplied string before using it to execute a system call. An attacker can leverage this vulnerability to execute code in the context of root.	N/A	A-CEN-CENT-190820/69

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Was ZDI-CAN-9721. **CVE ID : CVE-2020-15607**		
Improper Neutralization of Special Elements used in an OS Command ('OS Command Injection')	28-Jul-20	10	This vulnerability allows remote attackers to execute arbitrary code on affected installations of CentOS Web Panel cwp-e17.0.9.8.923. Authentication is not required to exploit this vulnerability. The specific flaw exists within ajax_dashboard.php. When parsing the ai_service parameter, the process does not properly validate a user-supplied string before using it to execute a system call. An attacker can leverage this vulnerability to execute code in the context of root. Was ZDI-CAN-9724. **CVE ID : CVE-2020-15608**	N/A	A-CEN-CENT-190820/70
Improper Neutralization of Special Elements used in an OS Command ('OS Command Injection')	28-Jul-20	10	This vulnerability allows remote attackers to execute arbitrary code on affected installations of CentOS Web Panel cwp-e17.0.9.8.923. Authentication is not required to exploit this vulnerability. The specific flaw exists within ajax_dashboard.php. When parsing the service_stop parameter, the process does not properly validate a user-supplied string before using it to execute a	N/A	A-CEN-CENT-190820/71

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			system call. An attacker can leverage this vulnerability to execute code in the context of root. Was ZDI-CAN-9726. **CVE ID : CVE-2020-15609**		
Improper Neutralization of Special Elements used in an OS Command ('OS Command Injection')	28-Jul-20	10	This vulnerability allows remote attackers to execute arbitrary code on affected installations of CentOS Web Panel cwp-e17.0.9.8.923. Authentication is not required to exploit this vulnerability. The specific flaw exists within ajax_php_pecl.php. When parsing the modulo parameter, the process does not properly validate a user-supplied string before using it to execute a system call. An attacker can leverage this vulnerability to execute code in the context of root. Was ZDI-CAN-9728. **CVE ID : CVE-2020-15610**	N/A	A-CEN-CENT-190820/72
Improper Neutralization of Special Elements used in an OS Command ('OS Command Injection')	28-Jul-20	10	This vulnerability allows remote attackers to execute arbitrary code on affected installations of CentOS Web Panel cwp-e17.0.9.8.923. Authentication is not required to exploit this vulnerability. The specific flaw exists within ajax_dashboard.php. When parsing the service_restart	N/A	A-CEN-CENT-190820/73

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			parameter, the process does not properly validate a user-supplied string before using it to execute a system call. An attacker can leverage this vulnerability to execute code in the context of root. Was ZDI-CAN-9734. **CVE ID : CVE-2020-15611**		
Improper Neutralization of Special Elements used in an OS Command ('OS Command Injection')	28-Jul-20	10	This vulnerability allows remote attackers to execute arbitrary code on affected installations of CentOS Web Panel cwp-e17.0.9.8.923. Authentication is not required to exploit this vulnerability. The specific flaw exists within ajax_ftp_manager.php. When parsing the userLogin parameter, the process does not properly validate a user-supplied string before using it to execute a system call. An attacker can leverage this vulnerability to execute code in the context of root. Was ZDI-CAN-9737. **CVE ID : CVE-2020-15612**	N/A	A-CEN-CENT-190820/74
Improper Neutralization of Special Elements used in an OS Command ('OS Command	28-Jul-20	10	This vulnerability allows remote attackers to execute arbitrary code on affected installations of CentOS Web Panel cwp-e17.0.9.8.923. Authentication is not required to exploit this	N/A	A-CEN-CENT-190820/75

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Injection')			vulnerability. The specific flaw exists within ajax_admin_apis.php. When parsing the line parameter, the process does not properly validate a user-supplied string before using it to execute a system call. An attacker can leverage this vulnerability to execute code in the context of root. Was ZDI-CAN-9739. **CVE ID : CVE-2020-15613**		
Improper Neutralization of Special Elements used in an OS Command ('OS Command Injection')	28-Jul-20	10	This vulnerability allows remote attackers to execute arbitrary code on affected installations of CentOS Web Panel cwp-e17.0.9.8.923. Authentication is not required to exploit this vulnerability. The specific flaw exists within ajax_php_pecl.php. When parsing the cha parameter, the process does not properly validate a user-supplied string before using it to execute a system call. An attacker can leverage this vulnerability to execute code in the context of root. Was ZDI-CAN-9718. **CVE ID : CVE-2020-15614**	N/A	A-CEN-CENT-190820/76
Improper Neutralization of Special Elements	28-Jul-20	10	This vulnerability allows remote attackers to execute arbitrary code on affected installations of	N/A	A-CEN-CENT-190820/77

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
used in an OS Command ('OS Command Injection')			CentOS Web Panel cwp-e17.0.9.8.923. Authentication is not required to exploit this vulnerability. The specific flaw exists within ajax_ftp_manager.php. The issue results from the lack of proper validation of a user-supplied string before using it to execute a system call. An attacker can leverage this vulnerability to execute code in the context of root. Was ZDI-CAN-9746. **CVE ID : CVE-2020-15615**		
Improper Neutralization of Special Elements used in an SQL Command ('SQL Injection')	28-Jul-20	7.8	This vulnerability allows remote attackers to disclose sensitive information on affected installations of CentOS Web Panel cwp-e17.0.9.8.923. Authentication is not required to exploit this vulnerability. The specific flaw exists within ajax_list_accounts.php. When parsing the package parameter, the process does not properly validate a user-supplied string before using it to construct SQL queries. An attacker can leverage this vulnerability to disclose information in the context of root. Was ZDI-CAN-9706.	N/A	A-CEN-CENT-190820/78

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2020-15616		
Improper Neutralization of Special Elements used in an SQL Command ('SQL Injection')	28-Jul-20	7.8	This vulnerability allows remote attackers to disclose sensitive information on affected installations of CentOS Web Panel cwp-e17.0.9.8.923. Authentication is not required to exploit this vulnerability. The specific flaw exists within ajax_list_accounts.php. When parsing the status parameter, the process does not properly validate a user-supplied string before using it to construct SQL queries. An attacker can leverage this vulnerability to disclose information in the context of root. Was ZDI-CAN-9708. **CVE ID : CVE-2020-15617**	N/A	A-CEN-CENT-190820/79
Improper Neutralization of Special Elements used in an SQL Command ('SQL Injection')	28-Jul-20	7.8	This vulnerability allows remote attackers to disclose sensitive information on affected installations of CentOS Web Panel cwp-e17.0.9.8.923. Authentication is not required to exploit this vulnerability. The specific flaw exists within ajax_list_accounts.php. When parsing the username parameter, the process does not properly	N/A	A-CEN-CENT-190820/80

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			validate a user-supplied string before using it to construct SQL queries. An attacker can leverage this vulnerability to disclose information in the context of root. Was ZDI-CAN-9717. **CVE ID : CVE-2020-15618**		
Improper Neutralization of Special Elements used in an SQL Command ('SQL Injection')	28-Jul-20	7.8	This vulnerability allows remote attackers to disclose sensitive information on affected installations of CentOS Web Panel cwp-e17.0.9.8.923. Authentication is not required to exploit this vulnerability. The specific flaw exists within ajax_list_accounts.php. When parsing the type parameter, the process does not properly validate a user-supplied string before using it to construct SQL queries. An attacker can leverage this vulnerability to disclose information in the context of root. Was ZDI-CAN-9723. **CVE ID : CVE-2020-15619**	N/A	A-CEN-CENT-190820/81
Improper Neutralization of Special Elements used in an SQL Command	28-Jul-20	7.8	This vulnerability allows remote attackers to disclose sensitive information on affected installations of CentOS Web Panel cwp-e17.0.9.8.923.	N/A	A-CEN-CENT-190820/82

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
('SQL Injection')			Authentication is not required to exploit this vulnerability. The specific flaw exists within ajax_list_accounts.php. When parsing the id parameter, the process does not properly validate a user-supplied string before using it to construct SQL queries. An attacker can leverage this vulnerability to disclose information in the context of root. Was ZDI-CAN-9741. **CVE ID : CVE-2020-15620**		
Improper Neutralization of Special Elements used in an SQL Command ('SQL Injection')	28-Jul-20	7.8	This vulnerability allows remote attackers to disclose sensitive information on affected installations of CentOS Web Panel cwp-e17.0.9.8.923. Authentication is not required to exploit this vulnerability. The specific flaw exists within ajax_mail_autoreply.php. When parsing the email parameter, the process does not properly validate a user-supplied string before using it to construct SQL queries. An attacker can leverage this vulnerability to disclose information in the context of root. Was ZDI-CAN-9711.	N/A	A-CEN-CENT-190820/83

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2020-15621		
Improper Neutralization of Special Elements used in an SQL Command ('SQL Injection')	28-Jul-20	7.8	This vulnerability allows remote attackers to disclose sensitive information on affected installations of CentOS Web Panel cwp-e17.0.9.8.923. Authentication is not required to exploit this vulnerability. The specific flaw exists within ajax_mail_autoreply.php. When parsing the search parameter, the process does not properly validate a user-supplied string before using it to construct SQL queries. An attacker can leverage this vulnerability to disclose information in the context of root. Was ZDI-CAN-9712. **CVE ID : CVE-2020-15622**	N/A	A-CEN-CENT-190820/84
Exposed Dangerous Method or Function	28-Jul-20	10	This vulnerability allows remote attackers to write arbitrary files on affected installations of CentOS Web Panel cwp-e17.0.9.8.923. Authentication is not required to exploit this vulnerability. The specific flaw exists within ajax_mod_security.php. When parsing the archivo parameter, the process does not properly validate a user-supplied path prior	N/A	A-CEN-CENT-190820/85

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			to using it in file operations. An attacker can leverage this vulnerability to execute code in the context of root. Was ZDI-CAN-9722. **CVE ID : CVE-2020-15623**		
Improper Neutralization of Special Elements used in an SQL Command ('SQL Injection')	28-Jul-20	7.8	This vulnerability allows remote attackers to disclose sensitive information on affected installations of CentOS Web Panel cwp-e17.0.9.8.923. Authentication is not required to exploit this vulnerability. The specific flaw exists within ajax_new_account.php. When parsing the domain parameter, the process does not properly validate a user-supplied string before using it to construct SQL queries. An attacker can leverage this vulnerability to disclose information in the context of root. Was ZDI-CAN-9727. **CVE ID : CVE-2020-15624**	N/A	A-CEN-CENT-190820/86
Improper Neutralization of Special Elements used in an SQL Command ('SQL Injection')	28-Jul-20	7.8	This vulnerability allows remote attackers to disclose sensitive information on affected installations of CentOS Web Panel cwp-e17.0.9.8.923. Authentication is not required to exploit this	N/A	A-CEN-CENT-190820/87

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			vulnerability. The specific flaw exists within ajax_add_mailbox.php. When parsing the username parameter, the process does not properly validate a user-supplied string before using it to construct SQL queries. An attacker can leverage this vulnerability to disclose information in the context of root. Was ZDI-CAN-9729. **CVE ID : CVE-2020-15625**		
Improper Neutralization of Special Elements used in an SQL Command ('SQL Injection')	28-Jul-20	7.8	This vulnerability allows remote attackers to disclose sensitive information on affected installations of CentOS Web Panel cwp-e17.0.9.8.923. Authentication is not required to exploit this vulnerability. The specific flaw exists within ajax_dashboard.php. When parsing the term parameter, the process does not properly validate a user-supplied string before using it to construct SQL queries. An attacker can leverage this vulnerability to disclose information in the context of root. Was ZDI-CAN-9730. **CVE ID : CVE-2020-15626**	N/A	A-CEN-CENT-190820/88
Improper	28-Jul-20	7.8	This vulnerability allows	N/A	A-CEN-CENT-

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Neutralization of Special Elements used in an SQL Command ('SQL Injection')			remote attackers to disclose sensitive information on affected installations of CentOS Web Panel cwp-e17.0.9.8.923. Authentication is not required to exploit this vulnerability. The specific flaw exists within ajax_mail_autoreply.php. When parsing the account parameter, the process does not properly validate a user-supplied string before using it to construct SQL queries. An attacker can leverage this vulnerability to disclose information in the context of root. Was ZDI-CAN-9738. **CVE ID : CVE-2020-15627**		190820/89
Improper Neutralization of Special Elements used in an SQL Command ('SQL Injection')	28-Jul-20	7.8	This vulnerability allows remote attackers to disclose sensitive information on affected installations of CentOS Web Panel cwp-e17.0.9.8.923. Authentication is not required to exploit this vulnerability. The specific flaw exists within ajax_mail_autoreply.php. When parsing the user parameter, the process does not properly validate a user-supplied string before using it to construct SQL queries. An attacker	N/A	A-CEN-CENT-190820/90

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			can leverage this vulnerability to disclose information in the context of root. Was ZDI-CAN-9710. **CVE ID : CVE-2020-15628**		
Cherokee-project					
cherokee					
NULL Pointer Dereference	27-Jul-20	5	Cherokee 0.4.27 to 1.2.104 is affected by a denial of service due to a NULL pointer dereferences. A remote unauthenticated attacker can crash the server by sending an HTTP request to protected resources using a malformed Authorization header that is mishandled during a cherokee_buffer_add call within cherokee_validator_parse_basic or cherokee_validator_parse_digest. **CVE ID : CVE-2020-12845**	N/A	A-CHE-CHER-190820/91
Cisco					
data_center_network_manager					
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	31-Jul-20	4.3	A vulnerability in the web-based management interface of Cisco Data Center Network Manager (DCNM) could allow an unauthenticated, remote attacker to conduct a cross-site scripting (XSS) attack against a user of the interface. The vulnerability	N/A	A-CIS-DATA-190820/92

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			exists because the web-based management interface does not properly validate user-supplied input. An attacker could exploit this vulnerability by intercepting a request from a user and injecting malicious data into an HTTP header. A successful exploit could allow the attacker to execute arbitrary script code in the context of the affected interface or access sensitive browser-based information. **CVE ID : CVE-2020-3460**		
Missing Authenticati on for Critical Function	31-Jul-20	5	A vulnerability in the web-based management interface of Cisco Data Center Network Manager (DCNM) could allow an unauthenticated, remote attacker to obtain confidential information from an affected device. The vulnerability is due to missing authentication on a specific part of the web-based management interface. An attacker could exploit this vulnerability by sending a crafted request to the interface. A successful exploit could allow the attacker to read confidential information	N/A	A-CIS-DATA-190820/93

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			from an affected device. **CVE ID : CVE-2020-3461**		
Improper Neutralization of Special Elements used in an SQL Command ('SQL Injection')	31-Jul-20	6.5	A vulnerability in the web-based management interface of Cisco Data Center Network Manager (DCNM) could allow an authenticated, remote attacker to conduct SQL injection attacks on an affected system. The vulnerability is due to improper validation of user-submitted parameters. An attacker could exploit this vulnerability by authenticating to the application and sending malicious requests to an affected system. A successful exploit could allow the attacker to obtain and modify sensitive information that is stored in the underlying database. **CVE ID : CVE-2020-3462**	N/A	A-CIS-DATA-190820/94
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	16-Jul-20	3.5	Multiple vulnerabilities in the web-based management interface of Cisco Data Center Network Manager (DCNM) could allow an authenticated, remote attacker to conduct a cross-site scripting (XSS) attack against a user of the interface on an affected device. These vulnerabilities are due to	N/A	A-CIS-DATA-190820/95

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			insufficient validation of user-supplied input by the web-based management interface. An attacker could exploit these vulnerabilities by persuading a user of the interface to click a customized link. A successful exploit could allow the attacker to execute arbitrary script code in the context of the interface or access sensitive browser-based information. **CVE ID : CVE-2020-3348**		
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	16-Jul-20	3.5	Multiple vulnerabilities in the web-based management interface of Cisco Data Center Network Manager (DCNM) could allow an authenticated, remote attacker to conduct a cross-site scripting (XSS) attack against a user of the interface on an affected device. These vulnerabilities are due to insufficient validation of user-supplied input by the web-based management interface. An attacker could exploit these vulnerabilities by persuading a user of the interface to click a customized link. A successful exploit could allow the attacker to execute arbitrary script	N/A	A-CIS-DATA-190820/96

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			code in the context of the interface or access sensitive browser-based information. **CVE ID : CVE-2020-3349**		
Missing Authenticati on for Critical Function	31-Jul-20	7.5	A vulnerability in the Device Manager application of Cisco Data Center Network Manager (DCNM) could allow an unauthenticated, remote attacker to bypass authentication and execute arbitrary actions on an affected device. The vulnerability is due to a failure in the software to perform proper authentication. An attacker could exploit this vulnerability by browsing to one of the hosted URLs in Cisco DCNM. A successful exploit could allow the attacker to interact with and use certain functions within the Cisco DCNM. **CVE ID : CVE-2020-3376**	N/A	A-CIS-DATA-190820/97
Improper Neutralizatio n of Special Elements used in an OS Command ('OS Command Injection')	31-Jul-20	6.5	A vulnerability in the Device Manager application of Cisco Data Center Network Manager (DCNM) could allow an authenticated, remote attacker to inject arbitrary commands on the affected device. The vulnerability is due to insufficient validation of user-supplied	N/A	A-CIS-DATA-190820/98

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			input. An attacker could exploit this vulnerability by sending crafted arguments to a specific field within the application. A successful exploit could allow the attacker to run commands as the administrator on the DCNM. **CVE ID : CVE-2020-3377**		
Argument Injection or Modification	16-Jul-20	7.2	A vulnerability in the CLI of Cisco Data Center Network Manager (DCNM) could allow an authenticated, local attacker to elevate privileges to root and execute arbitrary commands on the underlying operating system. The vulnerability is due to insufficient restrictions during the execution of an affected CLI command. An attacker could exploit this vulnerability by authenticating as the fmserver user and submitting malicious input to a specific command. A successful exploit could allow the attacker to elevate privileges to root and execute arbitrary commands on the underlying operating system. **CVE ID : CVE-2020-3380**	N/A	A-CIS-DATA-190820/99

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Use of Hard-coded Credentials	31-Jul-20	10	A vulnerability in the REST API of Cisco Data Center Network Manager (DCNM) could allow an unauthenticated, remote attacker to bypass authentication and execute arbitrary actions with administrative privileges on an affected device. The vulnerability exists because different installations share a static encryption key. An attacker could exploit this vulnerability by using the static key to craft a valid session token. A successful exploit could allow the attacker to perform arbitrary actions through the REST API with administrative privileges. **CVE ID : CVE-2020-3382**	N/A	A-CIS-DATA-190820/100
Improper Limitation of a Pathname to a Restricted Directory ('Path Traversal')	31-Jul-20	9	A vulnerability in the archive utility of Cisco Data Center Network Manager (DCNM) could allow an authenticated, remote attacker to conduct directory traversal attacks on an affected device. The vulnerability is due to a lack of proper input validation of paths that are embedded within archive files. An attacker could exploit this vulnerability by sending a crafted request to an affected device. A successful exploit	N/A	A-CIS-DATA-190820/101

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			could allow the attacker to write arbitrary files in the system with the privileges of the logged-in user. **CVE ID : CVE-2020-3383**		
N/A	31-Jul-20	6	A vulnerability in specific REST API endpoints of Cisco Data Center Network Manager (DCNM) could allow an authenticated, remote attacker to inject arbitrary commands on the underlying operating system with the privileges of the logged-in user. The vulnerability is due to insufficient validation of user-supplied input to the API. An attacker could exploit this vulnerability by sending a crafted request to the API. A successful exploit could allow the attacker to inject arbitrary commands on the underlying operating system. **CVE ID : CVE-2020-3384**	N/A	A-CIS-DATA-190820/102
Incorrect Authorization	31-Jul-20	9	A vulnerability in the REST API endpoint of Cisco Data Center Network Manager (DCNM) could allow an authenticated, remote attacker with a low-privileged account to bypass authorization on the API of an affected device. The vulnerability is due to insufficient authorization of certain	N/A	A-CIS-DATA-190820/103

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			API functions. An attacker could exploit this vulnerability by sending a crafted request to the API using low-privileged credentials. A successful exploit could allow the attacker to perform arbitrary actions through the REST API with administrative privileges. **CVE ID : CVE-2020-3386**		
sd-wan					
Insufficiently Protected Credentials	16-Jul-20	7.2	A vulnerability in Cisco SD-WAN Solution Software could allow an unauthenticated, local attacker to access an affected device by using an account that has a default, static password. This account has root privileges. The vulnerability exists because the affected software has a user account with a default, static password. An attacker could exploit this vulnerability by remotely connecting to an affected system by using this account. A successful exploit could allow the attacker to log in by using this account with root privileges. **CVE ID : CVE-2020-3180**	N/A	A-CIS-SD-W-190820/104
Incorrect Authorizatio	31-Jul-20	9	A vulnerability in the web-based management	N/A	A-CIS-SD-W-

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
n			interface of Cisco SD-WAN vManage Software could allow an authenticated, remote attacker to bypass authorization, enabling them to access sensitive information, modify the system configuration, or impact the availability of the affected system. The vulnerability is due to insufficient authorization checking on the affected system. An attacker could exploit this vulnerability by sending crafted HTTP requests to the web-based management interface of an affected system. A successful exploit could allow the attacker to gain privileges beyond what would normally be authorized for their configured user authorization level. The attacker may be able to access sensitive information, modify the system configuration, or impact the availability of the affected system. **CVE ID : CVE-2020-3374**		190820/105
Improper Restriction of Operations within the Bounds of a Memory	31-Jul-20	10	A vulnerability in Cisco SD-WAN Solution Software could allow an unauthenticated, remote attacker to cause a buffer overflow on an affected device. The vulnerability is due to insufficient input	N/A	A-CIS-SD-W-190820/106

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Buffer			validation. An attacker could exploit this vulnerability by sending crafted traffic to an affected device. A successful exploit could allow the attacker to gain access to information that they are not authorized to access, make changes to the system that they are not authorized to make, and execute commands on an affected system with privileges of the root user. **CVE ID : CVE-2020-3375**		
adaptive_security_appliance					
Improper Input Validation	22-Jul-20	5	A vulnerability in the web services interface of Cisco Adaptive Security Appliance (ASA) Software and Cisco Firepower Threat Defense (FTD) Software could allow an unauthenticated, remote attacker to conduct directory traversal attacks and read sensitive files on a targeted system. The vulnerability is due to a lack of proper input validation of URLs in HTTP requests processed by an affected device. An attacker could exploit this vulnerability by sending a crafted HTTP request containing directory traversal character sequences to an affected	N/A	A-CIS-ADAP-190820/107

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			device. A successful exploit could allow the attacker to view arbitrary files within the web services file system on the targeted device. The web services file system is enabled when the affected device is configured with either WebVPN or AnyConnect features. This vulnerability cannot be used to obtain access to ASA or FTD system files or underlying operating system (OS) files. **CVE ID : CVE-2020-3452**		
email_security_appliance					
Improper Input Validation	16-Jul-20	5	A vulnerability in URL filtering of Cisco Content Security Management Appliance (SMA) could allow an unauthenticated, remote attacker to bypass URL filtering on an affected device. The vulnerability is due to insufficient input validation. An attacker could exploit this vulnerability by sending a crafted, malicious HTTP request to an affected device. A successful exploit could allow the attacker to redirect users to malicious sites. **CVE ID : CVE-2020-3370**	N/A	A-CIS-EMAI-190820/108
webex_meetings_server					

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Improper Input Validation	16-Jul-20	4.3	A vulnerability in certain web pages of Cisco Webex Meetings and Cisco Webex Meetings Server could allow an unauthenticated, remote attacker to modify a web page in the context of a browser. The vulnerability is due to improper checks on parameter values within affected pages. An attacker could exploit this vulnerability by persuading a user to follow a crafted link that is designed to pass HTML code into an affected parameter. A successful exploit could allow the attacker to alter the contents of a web page to redirect the user to potentially malicious web sites, or the attacker could leverage this vulnerability to conduct further client-side attacks. **CVE ID : CVE-2020-3345**	N/A	A-CIS-WEBE-190820/109
vision_dynamic_signage_director					
Improper Neutralization of Special Elements used in an SQL Command ('SQL Injection')	16-Jul-20	4	A vulnerability in the web-based management interface of Cisco Vision Dynamic Signage Director could allow an authenticated, remote attacker with administrative credentials to conduct SQL injection attacks on an affected	N/A	A-CIS-VISI-190820/110

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			system. The vulnerability is due to improper validation of user-submitted parameters. An attacker could exploit this vulnerability by authenticating to the web-based management interface and sending malicious requests to an affected system. A successful exploit could allow the attacker to obtain data that is stored in the underlying database, including hashed user credentials. To exploit this vulnerability, an attacker would need valid administrative credentials. **CVE ID : CVE-2020-3450**		
prime_license_manager					
Incorrect Authorization	16-Jul-20	10	A vulnerability in the web management interface of Cisco Prime License Manager (PLM) Software could allow an unauthenticated, remote attacker to gain unauthorized access to an affected device. The vulnerability is due to insufficient validation of user input on the web management interface. An attacker could exploit this vulnerability by submitting a malicious request to an affected system. An exploit could	N/A	A-CIS-PRIM-190820/111

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			allow the attacker to gain administrative-level privileges on the system. The attacker needs a valid username to exploit this vulnerability. **CVE ID : CVE-2020-3140**		
vedge_cloud_router					
Uncontrolled Resource Consumption	16-Jul-20	7.8	A vulnerability in Cisco SD-WAN Solution Software could allow an unauthenticated, remote attacker to cause a denial of service (DoS) condition. The vulnerability is due to improper validation of fields in Cisco SD-WAN peering messages that are encapsulated in UDP packets. An attacker could exploit this vulnerability by sending crafted UDP messages to the targeted system. A successful exploit could allow the attacker to cause services on the device to fail, resulting in a DoS condition that could impact the targeted device and other devices that depend on it. **CVE ID : CVE-2020-3351**	N/A	A-CIS-VEDG-190820/112
N/A	16-Jul-20	7.8	A vulnerability in the deep packet inspection (DPI) engine of Cisco SD-WAN vEdge Routers could allow an unauthenticated, remote attacker to cause a denial of service (DoS)	N/A	A-CIS-VEDG-190820/113

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			condition on an affected device. The vulnerability is due to improper processing of FTP traffic. An attacker could exploit this vulnerability by sending crafted FTP packets through an affected device. A successful exploit could allow the attacker to make the device reboot continuously, causing a DoS condition. **CVE ID : CVE-2020-3369**		
N/A	16-Jul-20	6.1	A vulnerability in the deep packet inspection (DPI) engine of Cisco SD-WAN vEdge Routers could allow an unauthenticated, adjacent attacker to cause a denial of service (DoS) condition on an affected system. The vulnerability is due to insufficient handling of malformed packets. An attacker could exploit this vulnerability by sending crafted packets through an affected device. A successful exploit could allow the attacker to cause the device to reboot, resulting in a DoS condition. **CVE ID : CVE-2020-3385**	N/A	A-CIS-VEDG-190820/114
vbond_orchestrator					
Improper Input	16-Jul-20	7.2	A vulnerability in Cisco SD-WAN Solution Software could allow an	N/A	A-CIS-VBON-190820/115

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Validation			authenticated, local attacker to elevate privileges to Administrator on the underlying operating system. The vulnerability is due to insufficient input validation. An attacker could exploit this vulnerability by sending a crafted request to an affected system. A successful exploit could allow the attacker to gain administrative privileges. **CVE ID : CVE-2020-3379**		
vsmart_controller					
Uncontrolled Resource Consumption	16-Jul-20	7.8	A vulnerability in Cisco SD-WAN Solution Software could allow an unauthenticated, remote attacker to cause a denial of service (DoS) condition. The vulnerability is due to improper validation of fields in Cisco SD-WAN peering messages that are encapsulated in UDP packets. An attacker could exploit this vulnerability by sending crafted UDP messages to the targeted system. A successful exploit could allow the attacker to cause services on the device to fail, resulting in a DoS condition that could impact the targeted device and other devices that	N/A	A-CIS-VSMA-190820/116

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			depend on it. **CVE ID : CVE-2020-3351**		
Improper Input Validation	16-Jul-20	7.2	A vulnerability in Cisco SD-WAN Solution Software could allow an authenticated, local attacker to elevate privileges to Administrator on the underlying operating system. The vulnerability is due to insufficient input validation. An attacker could exploit this vulnerability by sending a crafted request to an affected system. A successful exploit could allow the attacker to gain administrative privileges. **CVE ID : CVE-2020-3379**	N/A	A-CIS-VSMA-190820/117
firepower_threat_defense					
Improper Input Validation	22-Jul-20	5	A vulnerability in the web services interface of Cisco Adaptive Security Appliance (ASA) Software and Cisco Firepower Threat Defense (FTD) Software could allow an unauthenticated, remote attacker to conduct directory traversal attacks and read sensitive files on a targeted system. The vulnerability is due to a lack of proper input validation of URLs in HTTP requests processed by an affected device. An attacker could exploit this	N/A	A-CIS-FIRE-190820/118

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			vulnerability by sending a crafted HTTP request containing directory traversal character sequences to an affected device. A successful exploit could allow the attacker to view arbitrary files within the web services file system on the targeted device. The web services file system is enabled when the affected device is configured with either WebVPN or AnyConnect features. This vulnerability cannot be used to obtain access to ASA or FTD system files or underlying operating system (OS) files. **CVE ID : CVE-2020-3452**		
meeting_server					
Improper Authenticati on	16-Jul-20	5	A vulnerability in the API subsystem of Cisco Meetings App could allow an unauthenticated, remote attacker to retain and reuse the Traversal Using Relay NAT (TURN) server credentials that are configured in an affected system. The vulnerability is due to insufficient protection mechanisms for the TURN server credentials. An attacker could exploit this vulnerability by intercepting the legitimate	N/A	A-CIS-MEET-190820/119

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			traffic that is generated by an affected system. An exploit could allow the attacker to obtain the TURN server credentials, which the attacker could use to place audio/video calls and forward packets through the configured TURN server. The attacker would not be able to take control of the TURN server unless the same credentials were used in multiple systems. **CVE ID : CVE-2020-3197**		
webex_meetings					
Improper Input Validation	16-Jul-20	4.3	A vulnerability in certain web pages of Cisco Webex Meetings and Cisco Webex Meetings Server could allow an unauthenticated, remote attacker to modify a web page in the context of a browser. The vulnerability is due to improper checks on parameter values within affected pages. An attacker could exploit this vulnerability by persuading a user to follow a crafted link that is designed to pass HTML code into an affected parameter. A successful exploit could allow the attacker to alter the contents of a web page to redirect the user to	N/A	A-CIS-WEBE-190820/120

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			potentially malicious web sites, or the attacker could leverage this vulnerability to conduct further client-side attacks. **CVE ID : CVE-2020-3345**		
Citrix					
workspace					
Improper Authentication	24-Jul-20	6	Improper access control in Citrix Workspace app for Windows 1912 CU1 and 2006.1 causes privilege escalation and code execution when the automatic updater service is running. **CVE ID : CVE-2020-8207**	N/A	A-CIT-WORK-190820/121
Clamav					
clamav					
NULL Pointer Dereference	20-Jul-20	5	A vulnerability in the EGG archive parsing module in Clam AntiVirus (ClamAV) Software versions 0.102.0 - 0.102.3 could allow an unauthenticated, remote attacker to cause a denial of service condition on an affected device. The vulnerability is due to a null pointer dereference. An attacker could exploit this vulnerability by sending a crafted EGG file to an affected device. An exploit could allow the attacker to cause the ClamAV scanning process crash, resulting in a denial	N/A	A-CLA-CLAM-190820/122

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			of service condition. **CVE ID : CVE-2020-3481**		
Claws-mail					
claws-mail					
Uncontrolled Recursion	28-Jul-20	5	In imap_scan_tree_recursive in Claws Mail through 3.17.6, a malicious IMAP server can trigger stack consumption because of unlimited recursion into subdirectories during a rebuild of the folder tree. **CVE ID : CVE-2020-16094**	N/A	A-CLA-CLAW-190820/123
N/A	23-Jul-20	7.5	common/session.c in Claws Mail before 3.17.6 has a protocol violation because suffix data after STARTTLS is mishandled. **CVE ID : CVE-2020-15917**	N/A	A-CLA-CLAW-190820/124
cloudfoundry					
cf-deployment					
Concurrent Execution using Shared Resource with Improper Synchronization ('Race Condition')	17-Jul-20	4.3	Go before 1.13.13 and 1.14.x before 1.14.5 has a data race in some net/http servers, as demonstrated by the httputil.ReverseProxy Handler, because it reads a request body and writes a response at the same time. **CVE ID : CVE-2020-15586**	https://groups.google.com/forum/#!topic/golang-announce/XZNfaiwgt2w, https://security.netapp.com/advisory/ntap-20200731-0005/, https://www.cloudfoundry.org/blog/cve-2020-	A-CLO-CF-D-190820/125

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
				15586/	
routing-release					
Concurrent Execution using Shared Resource with Improper Synchronization ('Race Condition')	17-Jul-20	4.3	Go before 1.13.13 and 1.14.x before 1.14.5 has a data race in some net/http servers, as demonstrated by the httputil.ReverseProxy Handler, because it reads a request body and writes a response at the same time. **CVE ID : CVE-2020-15586**	https://groups.google.com/forum/#!topic/golang-announce/XZNfaiwgt2w, https://security.netapp.com/advisory/ntap-20200731-0005/, https://www.cloudfoundry.org/blog/cve-2020-15586/	A-CLO-ROUT-190820/126
codecov					
codecov					
Improper Neutralization of Special Elements used in an OS Command ('OS Command Injection')	20-Jul-20	6.8	In codecov (npm package) before version 3.7.1 the upload method has a command injection vulnerability. Clients of the codecov-node library are unlikely to be aware of this, so they might unwittingly write code that contains a vulnerability. A similar CVE (CVE-2020-7597 for GHSA-5q88-cjfq-g2mh) was issued but the fix was incomplete. It only blocked &, and command injection is still possible using backticks instead to bypass the sanitizer. The	https://github.com/codecov/codecov-node/security/advisories/GHSA-xp63-6vf5-xf3v	A-COD-CODE-190820/127

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			attack surface is low in this case. Particularly in the standard use of codecov, where the module is used directly in a build pipeline, not built against as a library in another application that may supply malicious input and perform command injection. **CVE ID : CVE-2020-15123**		
Codesys					
control_for_plcnext					
Allocation of Resources Without Limits or Throttling	22-Jul-20	5	CODESYS Control runtime system before 3.5.16.10 allows Uncontrolled Memory Allocation. **CVE ID : CVE-2020-15806**	https://customers.codesys.com/index.php?eID=dumpFile&t=f&f=13199&token=3e283c3e73fed61f7c181a7fa1169477efaf0c58&download=	A-COD-CONT-190820/128
control_for_wago_touch_panels_600					
Allocation of Resources Without Limits or Throttling	22-Jul-20	5	CODESYS Control runtime system before 3.5.16.10 allows Uncontrolled Memory Allocation. **CVE ID : CVE-2020-15806**	https://customers.codesys.com/index.php?eID=dumpFile&t=f&f=13199&token=3e283c3e73fed61f7c181a7fa1169477efaf0c58&download=	A-COD-CONT-190820/129
control_for_beaglebone					

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Allocation of Resources Without Limits or Throttling	22-Jul-20	5	CODESYS Control runtime system before 3.5.16.10 allows Uncontrolled Memory Allocation. **CVE ID : CVE-2020-15806**	https://customers.codesys.com/index.php?eID=dumpFile&t=f&f=13199&token=3e283c3e73fed61f7c181a7fa1169477efaf0c58&download=	A-COD-CONT-190820/130
control_for_empc-a\/imx6					
Allocation of Resources Without Limits or Throttling	22-Jul-20	5	CODESYS Control runtime system before 3.5.16.10 allows Uncontrolled Memory Allocation. **CVE ID : CVE-2020-15806**	https://customers.codesys.com/index.php?eID=dumpFile&t=f&f=13199&token=3e283c3e73fed61f7c181a7fa1169477efaf0c58&download=	A-COD-CONT-190820/131
control_for_iot2000					
Allocation of Resources Without Limits or Throttling	22-Jul-20	5	CODESYS Control runtime system before 3.5.16.10 allows Uncontrolled Memory Allocation. **CVE ID : CVE-2020-15806**	https://customers.codesys.com/index.php?eID=dumpFile&t=f&f=13199&token=3e283c3e73fed61f7c181a7fa1169477efaf0c58&download=	A-COD-CONT-190820/132
control_for_linux					
Allocation of Resources Without	22-Jul-20	5	CODESYS Control runtime system before 3.5.16.10 allows Uncontrolled	https://customers.codesys.com/index.p	A-COD-CONT-190820/133

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Limits or Throttling			Memory Allocation. **CVE ID : CVE-2020-15806**	hp?eID=dumpFile&t=f&f=13199&token=3e283c3e73fed61f7c181a7fa1169477efaf0c58&download=	
control_for_pfc100					
Allocation of Resources Without Limits or Throttling	22-Jul-20	5	CODESYS Control runtime system before 3.5.16.10 allows Uncontrolled Memory Allocation. **CVE ID : CVE-2020-15806**	https://customers.codesys.com/index.php?eID=dumpFile&t=f&f=13199&token=3e283c3e73fed61f7c181a7fa1169477efaf0c58&download=	A-COD-CONT-190820/134
control_for_pfc200					
Allocation of Resources Without Limits or Throttling	22-Jul-20	5	CODESYS Control runtime system before 3.5.16.10 allows Uncontrolled Memory Allocation. **CVE ID : CVE-2020-15806**	https://customers.codesys.com/index.php?eID=dumpFile&t=f&f=13199&token=3e283c3e73fed61f7c181a7fa1169477efaf0c58&download=	A-COD-CONT-190820/135
control_for_raspberry_pi					
Allocation of Resources Without Limits or Throttling	22-Jul-20	5	CODESYS Control runtime system before 3.5.16.10 allows Uncontrolled Memory Allocation. **CVE ID : CVE-2020-15806**	https://customers.codesys.com/index.php?eID=dumpFile&t=f&f=13199&toke	A-COD-CONT-190820/136

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
				n=3e283c3e73fed61f7c181a7fa1169477efaf0c58&download=	
control_rte					
Allocation of Resources Without Limits or Throttling	22-Jul-20	5	CODESYS Control runtime system before 3.5.16.10 allows Uncontrolled Memory Allocation. **CVE ID : CVE-2020-15806**	https://customers.codesys.com/index.php?eID=dumpFile&t=f&f=13199&token=3e283c3e73fed61f7c181a7fa1169477efaf0c58&download=	A-COD-CONT-190820/137
control_runtime_system_toolkit					
Allocation of Resources Without Limits or Throttling	22-Jul-20	5	CODESYS Control runtime system before 3.5.16.10 allows Uncontrolled Memory Allocation. **CVE ID : CVE-2020-15806**	https://customers.codesys.com/index.php?eID=dumpFile&t=f&f=13199&token=3e283c3e73fed61f7c181a7fa1169477efaf0c58&download=	A-COD-CONT-190820/138
control_win					
Allocation of Resources Without Limits or Throttling	22-Jul-20	5	CODESYS Control runtime system before 3.5.16.10 allows Uncontrolled Memory Allocation. **CVE ID : CVE-2020-15806**	https://customers.codesys.com/index.php?eID=dumpFile&t=f&f=13199&token=3e283c3e73fed61f7c181a7fa11694	A-COD-CONT-190820/139

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
				77efaf0c58&download=	
embedded_target_visu_toolkit					
Allocation of Resources Without Limits or Throttling	22-Jul-20	5	CODESYS Control runtime system before 3.5.16.10 allows Uncontrolled Memory Allocation. **CVE ID : CVE-2020-15806**	https://customers.codesys.com/index.php?eID=dumpFile&t=f&f=13199&token=3e283c3e73fed61f7c181a7fa1169477efaf0c58&download=	A-COD-EMBE-190820/140
hmi					
Allocation of Resources Without Limits or Throttling	22-Jul-20	5	CODESYS Control runtime system before 3.5.16.10 allows Uncontrolled Memory Allocation. **CVE ID : CVE-2020-15806**	https://customers.codesys.com/index.php?eID=dumpFile&t=f&f=13199&token=3e283c3e73fed61f7c181a7fa1169477efaf0c58&download=	A-COD-HMI-190820/141
remote_target_visu_toolkit					
Allocation of Resources Without Limits or Throttling	22-Jul-20	5	CODESYS Control runtime system before 3.5.16.10 allows Uncontrolled Memory Allocation. **CVE ID : CVE-2020-15806**	https://customers.codesys.com/index.php?eID=dumpFile&t=f&f=13199&token=3e283c3e73fed61f7c181a7fa1169477efaf0c58&download=	A-COD-REMO-190820/142
simulation_runtime					

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Allocation of Resources Without Limits or Throttling	22-Jul-20	5	CODESYS Control runtime system before 3.5.16.10 allows Uncontrolled Memory Allocation. **CVE ID : CVE-2020-15806**	https://customers.codesys.com/index.php?eID=dumpFile&t=f&f=13199&token=3e283c3e73fed61f7c181a7fa1169477efaf0c58&download=	A-COD-SIMU-190820/143
collaboraoffice					
collabora_online_development_edition					
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	21-Jul-20	4.3	The WOPI API integration for Vereign Collabora CODE through 4.2.2 does not properly restrict delivery of JavaScript to a victim's browser, and lacks proper MIME type access control, which could lead to XSS that steals account credentials via cookies or local storage. The attacker must first obtain an API access token, which can be accomplished if the attacker is able to upload a .docx or .odt file. The associated API endpoints for exploitation are /wopi/files and /wopi/getAccessToken. **CVE ID : CVE-2020-12432**	N/A	A-COL-COLL-190820/144
Concrete5					
concrete5					
Unrestricted Upload of File with	28-Jul-20	9	Concrete5 before 8.5.3 allows Unrestricted Upload of File with	https://github.com/concrete5/concret	A-CON-CONC-190820/145

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Dangerous Type			Dangerous Type such as a .phar file. **CVE ID : CVE-2020-11476**	e5/pull/8713, https://github.com/concrete5/concrete5/releases/tag/8.5.3	
connectwise					
automate					
Improper Authentication	16-Jul-20	7.5	ConnectWise Automate through 2020.x has insufficient validation on certain authentication paths, allowing authentication bypass via a series of attempts. This was patched in 2020.7 and in a hotfix for 2019.12. **CVE ID : CVE-2020-15027**	N/A	A-CON-AUTO-190820/146
containous					
traefik					
URL Redirection to Untrusted Site ('Open Redirect')	30-Jul-20	4	In Traefik before versions 1.7.26, 2.2.8, and 2.3.0-rc3, there exists a potential open redirect vulnerability in Traefik's handling of the "X-Forwarded-Prefix" header. The Traefik API dashboard component doesn't validate that the value of the header "X-Forwarded-Prefix" is a site relative path and will redirect to any header provided URI. Successful exploitation of an open redirect can be used to entice victims to disclose sensitive information.	https://github.com/containous/traefik/security/advisories/GHSA-6qq8-5wq3-86rp	A-CON-TRAE-190820/147

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Active Exploitation of this issue is unlikely as it would require active header injection, however the Traefik team addressed this issue nonetheless to prevent abuse in e.g. cache poisoning scenarios. **CVE ID : CVE-2020-15129**		
Dell					
emc_openmanage_server_administrator					
Improper Limitation of a Pathname to a Restricted Directory ('Path Traversal')	28-Jul-20	6.4	Dell EMC OpenManage Server Administrator (OMSA) versions 9.4 and prior contain multiple path traversal vulnerabilities. An unauthenticated remote attacker could potentially exploit these vulnerabilities by sending a crafted Web API request containing directory traversal character sequences to gain file system access on the compromised management station. **CVE ID : CVE-2020-5377**	N/A	A-DEL-EMC_-190820/148
devspace					
devspace					
Improper Authentication	23-Jul-20	7.5	The UI in DevSpace 4.13.0 allows web sites to execute actions on pods (on behalf of a victim) because of a lack of authentication for the WebSocket protocol. This leads to remote code	https://github.com/devspace-cloud/devspace/releases/tag/v4.14.0	A-DEV-DEVS-190820/149

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			execution. **CVE ID : CVE-2020-15391**		
docsifyjs					
docsify					
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	20-Jul-20	4.3	docsify prior to 4.11.4 is susceptible to Cross-site Scripting (XSS). Docsify.js uses fragment identifiers (parameters after # sign) to load resources from server-side .md files. Due to lack of validation here, it is possible to provide external URLs after the /#/ (domain.com/#//attacker.com) and render arbitrary JavaScript/HTML inside docsify page. **CVE ID : CVE-2020-7680**	N/A	A-DOC-DOCS-190820/150
dp3t-backend-software_development_kit_project					
dp3t-backend-software_development_kit					
Improper Verification of Cryptographic Signature	30-Jul-20	5	An issue was discovered in DP3T-Backend-SDK before 1.1.1 for Decentralised Privacy-Preserving Proximity Tracing (DP3T). When it is configured to check JWT before uploading/publishing keys, it is possible to skip the signature check by providing a JWT token with alg=none. **CVE ID : CVE-2020-15957**	N/A	A-DP3-DP3T-190820/151
duo					
duoconnect					

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Cleartext Transmission of Sensitive Information	20-Jul-20	2.9	The DuoConnect client enables users to establish SSH connections to hosts protected by a DNG instance. When a user initiates an SSH connection to a DNG-protected host for the first time using DuoConnect, the userâ€™s browser is opened to a login screen in order to complete authentication determined by the contents of the '-relay' argument. If the â€˜-relayâ€™ is set to a URL beginning with "http://", then the browser will initially attempt to load the URL over an insecure HTTP connection, before being immediately redirected to HTTPS (in addition to standard redirect mechanisms, the DNG uses HTTP Strict Transport Security headers to enforce this). After successfully authenticating to a DNG, DuoConnect stores an authentication token in a local system cache, so users do not have to complete this browser-based authentication workflow for every subsequent SSH connection. These tokens are valid for a configurable period of time, which	N/A	A-DUO-DUOC-190820/152

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			defaults to 8 hours. If a user running DuoConnect already has a valid token, then instead of opening a web browser, DuoConnect directly contacts the DNG, again using the configured '-relay' value, and sends this token, as well as the intended SSH server hostname and port numbers. If the '-relay' argument begins with "http://", then this request will be sent over an insecure connection, and could be exposed to an attacker who is sniffing the traffic on the same network. The DNG authentication tokens that may be exposed during SSH relay may be used to gain network-level access to the servers and ports protected by that given relay host. The DNG provides network-level access only to the protected SSH servers. It does not interact with the independent SSH authentication and encryption. An attacker cannot use a stolen token on its own to authenticate against a DNG-protected SSH server. **CVE ID : CVE-2020-3442**		
Elasticsearch					

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
kibana					
Incorrect Comparison	27-Jul-20	4.3	Kibana versions before 6.8.11 and 7.8.1 contain a denial of service (DoS) flaw in Timelion. An attacker can construct a URL that when viewed by a Kibana user can lead to the Kibana process consuming large amounts of CPU and becoming unresponsive. **CVE ID : CVE-2020-7016**	N/A	A-ELA-KIBA-190820/153
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	27-Jul-20	3.5	In Kibana versions before 6.8.11 and 7.8.1 the region map visualization in contains a stored XSS flaw. An attacker who is able to edit or create a region map visualization could obtain sensitive information or perform destructive actions on behalf of Kibana users who view the region map visualization. **CVE ID : CVE-2020-7017**	N/A	A-ELA-KIBA-190820/154
Embedthis					
goahead					
Authentication Bypass by Capture-replay	23-Jul-20	6.8	The HTTP Digest Authentication in the GoAhead web server before 5.1.2 does not completely protect against replay attacks. This allows an unauthenticated remote attacker to bypass authentication via capture-replay if TLS is not used to protect the underlying	N/A	A-EMB-GOAH-190820/155

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			communication channel. **CVE ID : CVE-2020-15688**		
encode					
uvicorn					
Improper Neutralization of Special Elements in Output Used by a Downstream Component ('Injection')	27-Jul-20	5	This affects all versions of package uvicorn. The request logger provided by the package is vulnerable to ASNI escape sequence injection. Whenever any HTTP request is received, the default behaviour of uvicorn is to log its details to either the console or a log file. When attackers request crafted URLs with percent-encoded escape sequences, the logging component will log the URL after it's been processed with urllib.parse.unquote, therefore converting any percent-encoded characters into their single-character equivalent, which can have special meaning in terminal emulators. By requesting URLs with crafted paths, attackers can: * Pollute uvicorn's access logs, therefore jeopardising the integrity of such files. * Use ANSI sequence codes to attempt to interact with the terminal emulator that's displaying the logs (either in real time or from a file).	N/A	A-ENC-UVIC-190820/156

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2020-7694		
Improper Neutralization of Special Elements in Output Used by a Downstream Component ('Injection')	27-Jul-20	5	Uvicorn before 0.11.7 is vulnerable to HTTP response splitting. CRLF sequences are not escaped in the value of HTTP headers. Attackers can exploit this to add arbitrary headers to HTTP responses, or even return an arbitrary response body, whenever crafted input is used to construct HTTP headers. **CVE ID : CVE-2020-7695**	N/A	A-ENC-UVIC-190820/157
espressif					
esp-idf					
Improper Authentication	23-Jul-20	4.3	An encryption-bypass issue was discovered on Espressif ESP-IDF devices through 4.2, ESP8266_NONOS_SDK devices through 3.0.3, and ESP8266_RTOS_SDK devices through 3.3. Broadcasting forged beacon frames forces a device to change its authentication mode to OPEN, effectively disabling its 802.11 encryption. **CVE ID : CVE-2020-12638**	N/A	A-ESP-ESP--190820/158
esp8266_nonos_sdk					
Improper Authentication	23-Jul-20	4.3	An encryption-bypass issue was discovered on Espressif ESP-IDF devices through 4.2, ESP8266_NONOS_SDK devices through 3.0.3, and	N/A	A-ESP-ESP8-190820/159

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			ESP8266_RTOS_SDK devices through 3.3. Broadcasting forged beacon frames forces a device to change its authentication mode to OPEN, effectively disabling its 802.11 encryption. **CVE ID : CVE-2020-12638**		
esp8266_rtos_sdk					
Improper Authentication	23-Jul-20	4.3	An encryption-bypass issue was discovered on Espressif ESP-IDF devices through 4.2, ESP8266_NONOS_SDK devices through 3.0.3, and ESP8266_RTOS_SDK devices through 3.3. Broadcasting forged beacon frames forces a device to change its authentication mode to OPEN, effectively disabling its 802.11 encryption. **CVE ID : CVE-2020-12638**	N/A	A-ESP-ESP8-190820/160
express-fileupload_project					
express-fileupload					
Improper Neutralization of Special Elements in Output Used by a Downstream Component ('Injection')	30-Jul-20	7.5	This affects the package express-fileupload before 1.1.8. If the parseNested option is enabled, sending a corrupt HTTP request can lead to denial of service or arbitrary code execution. **CVE ID : CVE-2020-7699**	https://github.com/richardgirges/express-fileupload/issues/236, https://snyk.io/vuln/SNYK-JS-EXPRESSFILEUPLOAD-595969	A-EXP-EXPR-190820/161

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
eyesurfer					
bflyinstallerx.ocx					
Download of Code Without Integrity Check	17-Jul-20	7.5	EyeSurfer BflyInstallerX.ocx v1.0.0.16 and earlier versions contain a vulnerability that could allow remote files to be download by setting the arguments to the vulnerable method. This can be leveraged for code execution. When the vulnerable method is called, they fail to properly check the parameters that are passed to it. **CVE ID : CVE-2020-7826**	https://www.boho.or.kr/krcert/secNoticeView.do?bulletin_writing_sequence=35512	A-EYE-BFLY-190820/162
fast-http_project					
fast-http					
Improper Limitation of a Pathname to a Restricted Directory ('Path Traversal')	25-Jul-20	5	This affects all versions of package fast-http. There is no path sanitization in the path provided at fs.readFile in index.js. **CVE ID : CVE-2020-7687**	N/A	A-FAS-FAST-190820/163
fastify					
fastify					
Uncontrolled Resource Consumption	30-Jul-20	4	A denial of service vulnerability exists in Fastify v2.14.1 and v3.0.0-rc.4 that allows a malicious user to trigger resource exhaustion (when the allErrors option is used) with specially crafted	N/A	A-FAS-FAST-190820/164

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			schemas. **CVE ID : CVE-2020-8192**		
faye_project					
faye					
Improper Certificate Validation	31-Jul-20	6.4	Faye before version 1.4.0, there is a lack of certification validation in TLS handshakes. Faye uses em-http-request and faye-websocket in the Ruby version of its client. Those libraries both use the `EM::Connection#start_tls` method in EventMachine to implement the TLS handshake whenever a `wss:` URL is used for the connection. This method does not implement certificate verification by default, meaning that it does not check that the server presents a valid and trusted TLS certificate for the expected hostname. That means that any `https:` or `wss:` connection made using these libraries is vulnerable to a man-in-the-middle attack, since it does not confirm the identity of the server it is connected to. The first request a Faye client makes is always sent via normal HTTP, but later messages may be sent via WebSocket. Therefore it is vulnerable to the same	https://github.com/faye/faye/security/advisories/GHSA-3q49-h8f9-9fr9	A-FAY-FAYE-190820/165

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			problem that these underlying libraries are, and we needed both libraries to support TLS verification before Faye could claim to do the same. Your client would still be insecure if its initial HTTPS request was verified, but later WebSocket connections were not. This is fixed in Faye v1.4.0, which enables verification by default. For further background information on this issue, please see the referenced GitHub Advisory. **CVE ID : CVE-2020-15134**		
faye-websocket_project					
faye-websocket					
Improper Certificate Validation	31-Jul-20	5.8	In faye-websocket before version 0.11.0, there is a lack of certification validation in TLS handshakes. The `Faye::WebSocket::Client` class uses the `EM::Connection#start_tls` method in EventMachine to implement the TLS handshake whenever a `wss:` URL is used for the connection. This method does not implement certificate verification by default, meaning that it does not check that the server presents a valid and trusted TLS certificate for	https://github.com/faye/faye-websocket-ruby/security/advisories/GHSA-2v5c-755p-p4gv	A-FAY-FAYE-190820/166

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			the expected hostname. That means that any `wss:` connection made using this library is vulnerable to a man-in-the-middle attack, since it does not confirm the identity of the server it is connected to. For further background information on this issue, please see the referenced GitHub Advisory. Upgrading `faye-websocket` to v0.11.0 is recommended. **CVE ID : CVE-2020-15133**		
flexera					
flexnet_publisher					
Information Exposure	31-Jul-20	5	An information disclosure vulnerability has been identified in FlexNet Publisher lmadmin.exe 11.14.0.2. The web portal link can be used to access to system files or other important files on the system. **CVE ID : CVE-2020-12081**	https://community.flexera.com/t5/FlexNet-Publisher-Knowledge-Base/CVE-2020-12081-Remediated-in-FlexNet-Publisher/ta-p/153505	A-FLE-FLEX-190820/167
freediameter					
freediameter					
Integer Underflow (Wrap or Wraparound)	28-Jul-20	5	An exploitable denial of service vulnerability exists in the freeDiameter functionality of freeDiameter 1.3.2. A specially crafted Diameter request can trigger a	N/A	A-FRE-FREE-190820/168

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			memory corruption resulting in denial-of-service. An attacker can send a malicious packet to trigger this vulnerability. **CVE ID : CVE-2020-6098**		
freemedsoftware					
openclinic_ga					
N/A	29-Jul-20	7.5	OpenClinic GA 5.09.02 contains a hidden default user account that may be accessed if an administrator has not expressly turned off this account, which may allow an attacker to login and execute arbitrary commands. **CVE ID : CVE-2020-14487**	N/A	A-FRE-OPEN-190820/169
Unrestricted Upload of File with Dangerous Type	29-Jul-20	9	OpenClinic GA 5.09.02 and 5.89.05b does not properly verify uploaded files, which may allow a low-privilege user to upload and execute arbitrary files on the system. **CVE ID : CVE-2020-14488**	N/A	A-FRE-OPEN-190820/170
freerdp					
freerdp					
Improper Input Validation	27-Jul-20	3.5	In FreeRDP less than or equal to 2.1.2, an integer overflow exists due to missing input sanitation in rdpegfx channel. All FreeRDP clients are affected. The input rectangles from the server are not checked against	https://github.com/FreeRDP/FreeRDP/security/advisories/GHSA-4r38-6hq7-j3j9	A-FRE-FREE-190820/171

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			local surface coordinates and blindly accepted. A malicious server can send data that will crash the client later on (invalid length arguments to a `memcpy`) This has been fixed in 2.2.0. As a workaround, stop using command line arguments /gfx, /gfx-h264 and /network:auto **CVE ID : CVE-2020-15103**		
Gambio					
gambio_gx					
Improper Neutralization of Special Elements used in an SQL Command ('SQL Injection')	28-Jul-20	4	Gambio GX before 4.0.1.0 allows SQL Injection in admin/gv_mail.php. **CVE ID : CVE-2020-10982**	N/A	A-GAM-GAMB-190820/172
Improper Neutralization of Special Elements used in an SQL Command ('SQL Injection')	28-Jul-20	4	Gambio GX before 4.0.1.0 allows SQL Injection in admin/mobile.php. **CVE ID : CVE-2020-10983**	N/A	A-GAM-GAMB-190820/173
Cross-Site Request Forgery (CSRF)	28-Jul-20	6.8	Gambio GX before 4.0.1.0 allows admin/admin.php CSRF. **CVE ID : CVE-2020-10984**	N/A	A-GAM-GAMB-190820/174
Improper Neutralizatio	28-Jul-20	3.5	Gambio GX before 4.0.1.0 allows XSS in	N/A	A-GAM-GAMB-

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
n of Input During Web Page Generation ('Cross-site Scripting')			admin/coupon_admin.php. **CVE ID : CVE-2020-10985**		190820/175
gerapy					
gerapy					
Improper Neutralization of Special Elements in Output Used by a Downstream Component ('Injection')	29-Jul-20	7.5	This affects the package Gerapy from 0 and before 0.9.3. The input being passed to Popen, via the project_configure endpoint, isn't being sanitized. **CVE ID : CVE-2020-7698**	N/A	A-GER-GERA-190820/176
Glpi-project					
glpi					
Improper Neutralization of Special Elements used in an SQL Command ('SQL Injection')	17-Jul-20	4	In glpi before 9.5.1, there is a SQL injection for all usages of "Clone" feature. This has been fixed in 9.5.1. **CVE ID : CVE-2020-15108**	https://github.com/glpi-project/glpi/security/advisories/GHSA-qv6w-68gq-wx2v	A-GLP-GLPI-190820/177
Gnome					
balsa					
NULL Pointer Dereference	29-Jul-20	5	In GNOME Balsa before 2.6.0, a malicious server operator or man in the middle can trigger a NULL pointer dereference and client crash by sending a PREAUTH response to imap_mbox_connect in	N/A	A-GNO-BALS-190820/178

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			libbalsa/imap/imap-handle.c. **CVE ID : CVE-2020-16118**		
evolution-data-server					
NULL Pointer Dereference	29-Jul-20	4.3	In GNOME evolution-data-server before 3.35.91, a malicious server can crash the mail client with a NULL pointer dereference by sending an invalid (e.g., minimal) CAPABILITY line on a connection attempt. This is related to imapx_free_capability and imapx_connect_to_server. **CVE ID : CVE-2020-16117**	N/A	A-GNO-EVOL-190820/179
Improper Neutralization of Special Elements in Output Used by a Downstream Component ('Injection')	17-Jul-20	4.3	evolution-data-server (eds) through 3.36.3 has a STARTTLS buffering issue that affects SMTP and POP3. When a server sends a "begin TLS" response, eds reads additional data and evaluates it in a TLS context, aka "response injection." **CVE ID : CVE-2020-14928**	https://bugzilla.suse.com/show_bug.cgi?id=1173910, https://gitlab.gnome.org/GNOME//evolution-data-server/commit/ba82be72cfd427b5d72ff21f929b3a6d8529c4df, https://lists.debian.org/debian-lts-announce/2020/07/msg00012.html	A-GNO-EVOL-190820/180
GNU					

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
grub2					
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	30-Jul-20	4.6	A flaw was found in grub2, prior to version 2.06. An attacker may use the GRUB 2 flaw to hijack and tamper the GRUB verification process. This flaw also allows the bypass of Secure Boot protections. In order to load an untrusted or modified kernel, an attacker would first need to establish access to the system such as gaining physical access, obtain the ability to alter a pxe-boot network, or have remote access to a networked system with root access. With this access, an attacker could then craft a string to cause a buffer overflow by injecting a malicious payload that leads to arbitrary code execution within GRUB. The highest threat from this vulnerability is to data confidentiality and integrity as well as system availability. **CVE ID : CVE-2020-10713**	https://security.netapp.com/advisory/ntap-20200731-0008/	A-GNU-GRUB-190820/181
Integer Overflow or Wraparound	29-Jul-20	4.4	In grub2 versions before 2.06 the grub memory allocator doesn't check for possible arithmetic overflows on the requested allocation size. This leads the function to	https://security.netapp.com/advisory/ntap-20200731-0008/	A-GNU-GRUB-190820/182

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			return invalid memory allocations which can be further used to cause possible integrity, confidentiality and availability impacts during the boot process. **CVE ID : CVE-2020-14308**		
Integer Overflow or Wraparound	30-Jul-20	4.6	There's an issue with grub2 in all versions before 2.06 when handling squashfs filesystems containing a symbolic link with name length of UINT32 bytes in size. The name size leads to an arithmetic overflow leading to a zero-size allocation further causing a heap-based buffer overflow with attacker controlled data. **CVE ID : CVE-2020-14309**	https://security.netapp.com/advisory/ntap-20200731-0008/	A-GNU-GRUB-190820/183
Out-of-bounds Write	31-Jul-20	3.6	There is an issue on grub2 before version 2.06 at function read_section_as_string(). It expects a font name to be at max UINT32_MAX - 1 length in bytes but it doesn't verify it before proceed with buffer allocation to read the value from the font value. An attacker may leverage that by crafting a malicious font file which has a name with UINT32_MAX, leading to read_section_as_string() to an arithmetic overflow,	https://bugzilla.redhat.com/show_bug.cgi?id=CVE-2020-14310	A-GNU-GRUB-190820/184

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			zero-sized allocation and further heap-based buffer overflow. **CVE ID : CVE-2020-14310**		
Out-of-bounds Write	31-Jul-20	3.6	There is an issue with grub2 before version 2.06 while handling symlink on ext filesystems. A filesystem containing a symbolic link with an inode size of UINT32_MAX causes an arithmetic overflow leading to a zero-sized memory allocation with subsequent heap-based buffer overflow. **CVE ID : CVE-2020-14311**	https://bugzilla.redhat.com/show_bug.cgi?id=CVE-2020-14311	A-GNU-GRUB-190820/185
Improper Verification of Cryptographic Signature	29-Jul-20	4.4	GRUB2 fails to validate kernel signature when booted directly without shim, allowing secure boot to be bypassed. This only affects systems where the kernel signing certificate has been imported directly into the secure boot database and the GRUB image is booted directly without the use of shim. This issue affects GRUB2 version 2.04 and prior versions. **CVE ID : CVE-2020-15705**	https://lists.gnu.org/archive/html/grub-devel/2020-07/msg00034.html, https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/ADV200011, https://security.netapp.com/advisory/ntap-20200731-0008/	A-GNU-GRUB-190820/186
Concurrent Execution using Shared	29-Jul-20	4.4	GRUB2 contains a race condition in grub_script_function_creat	https://lists.gnu.org/archive/html/gru	A-GNU-GRUB-190820/187

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Resource with Improper Synchronization ('Race Condition')			e() leading to a use-after-free vulnerability which can be triggered by redefining a function whilst the same function is already executing, leading to arbitrary code execution and secure boot restriction bypass. This issue affects GRUB2 version 2.04 and prior versions. **CVE ID : CVE-2020-15706**	b-devel/2020-07/msg00034.html, https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/ADV200011, https://security.netapp.com/advisory/ntap-20200731-0008/	
Concurrent Execution using Shared Resource with Improper Synchronization ('Race Condition')	29-Jul-20	4.4	Integer overflows were discovered in the functions grub_cmd_initrd and grub_initrd_init in the efilinux component of GRUB2, as shipped in Debian, Red Hat, and Ubuntu (the functionality is not included in GRUB2 upstream), leading to a heap-based buffer overflow. These could be triggered by an extremely large number of arguments to the initrd command on 32-bit architectures, or a crafted filesystem with very large files on any architecture. An attacker could use this to execute arbitrary code and bypass UEFI Secure Boot restrictions. This issue affects GRUB2	https://lists.gnu.org/archive/html/grub-devel/2020-07/msg00034.html, https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/ADV200011, https://security.netapp.com/advisory/ntap-20200731-0008/	A-GNU-GRUB-190820/188

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			version 2.04 and prior versions. **CVE ID : CVE-2020-15707**		
libredwg					
NULL Pointer Dereference	17-Jul-20	4.3	GNU LibreDWG before 0.11 allows NULL pointer dereferences via crafted input files. **CVE ID : CVE-2020-15807**	N/A	A-GNU-LIBR-190820/189
gofiber					
fiber					
Improper Neutralization of Special Elements in Output Used by a Downstream Component ('Injection')	20-Jul-20	5.8	In Fiber before version 1.12.6, the filename that is given in c.Attachment() (https://docs.gofiber.io/ctx#attachment) is not escaped, and therefore vulnerable for a CRLF injection attack. I.e. an attacker could upload a custom filename and then give the link to the victim. With this filename, the attacker can change the name of the downloaded file, redirect to another site, change the authorization header, etc. A possible workaround is to serialize the input before passing it to ctx.Attachment(). **CVE ID : CVE-2020-15111**	https://github.com/gofiber/fiber/security/advisories/GHSA-9cx9-x2gp-9qvh	A-GOF-FIBE-190820/190
Golang					
go					
Improper Certificate	17-Jul-20	5	In Go before 1.13.13 and 1.14.x before 1.14.5, Certificate.Verify may lack	https://groups.google.com/forum/#!t	A-GOL-GO-190820/191

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Validation			a check on the VerifyOptions.KeyUsages EKU requirements (if VerifyOptions.Roots equals nil and the installation is on Windows). Thus, X.509 certificate verification is incomplete. **CVE ID : CVE-2020-14039**	opic/golang-announce/XZNfaiwgt2w, https://security.netapp.com/advisory/ntap-20200731-0005/	
Concurrent Execution using Shared Resource with Improper Synchronization ('Race Condition')	17-Jul-20	4.3	Go before 1.13.13 and 1.14.x before 1.14.5 has a data race in some net/http servers, as demonstrated by the httputil.ReverseProxy Handler, because it reads a request body and writes a response at the same time. **CVE ID : CVE-2020-15586**	https://groups.google.com/forum/#!topic/golang-announce/XZNfaiwgt2w, https://security.netapp.com/advisory/ntap-20200731-0005/, https://www.cloudfoundry.org/blog/cve-2020-15586/	A-GOL-GO-190820/192
Google					
chrome					
Use After Free	22-Jul-20	6.8	Use after free in speech in Google Chrome prior to 83.0.4103.106 allowed a remote attacker to potentially perform a sandbox escape via a crafted HTML page. **CVE ID : CVE-2020-6505**	N/A	A-GOO-CHRO-190820/193
Incorrect Authorization	22-Jul-20	4.3	Insufficient policy enforcement in WebView in Google Chrome on	N/A	A-GOO-CHRO-190820/194

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Android prior to 83.0.4103.106 allowed a remote attacker to bypass site isolation via a crafted HTML page. **CVE ID : CVE-2020-6506**		
Out-of-bounds Write	22-Jul-20	6.8	Out of bounds write in V8 in Google Chrome prior to 83.0.4103.106 allowed a remote attacker to potentially exploit heap corruption via a crafted HTML page. **CVE ID : CVE-2020-6507**	N/A	A-GOO-CHRO-190820/195
Use After Free	22-Jul-20	6.8	Use after free in extensions in Google Chrome prior to 83.0.4103.116 allowed an attacker who convinced a user to install a malicious extension to potentially perform a sandbox escape via a crafted Chrome Extension. **CVE ID : CVE-2020-6509**	N/A	A-GOO-CHRO-190820/196
Out-of-bounds Write	22-Jul-20	6.8	Heap buffer overflow in background fetch in Google Chrome prior to 84.0.4147.89 allowed a remote attacker to potentially exploit heap corruption via a crafted HTML page. **CVE ID : CVE-2020-6510**	N/A	A-GOO-CHRO-190820/197
Information Exposure	22-Jul-20	4.3	Information leak in content security policy in Google Chrome prior to 84.0.4147.89 allowed a remote attacker to leak cross-origin data via a	N/A	A-GOO-CHRO-190820/198

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			crafted HTML page. **CVE ID : CVE-2020-6511**		
Access of Resource Using Incompatible Type ('Type Confusion')	22-Jul-20	9.3	Type Confusion in V8 in Google Chrome prior to 84.0.4147.89 allowed a remote attacker to potentially exploit heap corruption via a crafted HTML page. **CVE ID : CVE-2020-6512**	N/A	A-GOO-CHRO-190820/199
Out-of-bounds Write	22-Jul-20	9.3	Heap buffer overflow in PDFium in Google Chrome prior to 84.0.4147.89 allowed a remote attacker to potentially exploit heap corruption via a crafted PDF file. **CVE ID : CVE-2020-6513**	N/A	A-GOO-CHRO-190820/200
N/A	22-Jul-20	4.3	Inappropriate implementation in WebRTC in Google Chrome prior to 84.0.4147.89 allowed an attacker in a privileged network position to potentially exploit heap corruption via a crafted SCTP stream. **CVE ID : CVE-2020-6514**	N/A	A-GOO-CHRO-190820/201
Use After Free	22-Jul-20	9.3	Use after free in tab strip in Google Chrome prior to 84.0.4147.89 allowed a remote attacker to potentially exploit heap corruption via a crafted HTML page. **CVE ID : CVE-2020-6515**	N/A	A-GOO-CHRO-190820/202
N/A	22-Jul-20	4.3	Policy bypass in CORS in Google Chrome prior to	N/A	A-GOO-CHRO-190820/203

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			84.0.4147.89 allowed a remote attacker to leak cross-origin data via a crafted HTML page. **CVE ID : CVE-2020-6516**		
Out-of-bounds Write	22-Jul-20	9.3	Heap buffer overflow in history in Google Chrome prior to 84.0.4147.89 allowed a remote attacker to potentially exploit heap corruption via a crafted HTML page. **CVE ID : CVE-2020-6517**	N/A	A-GOO-CHRO-190820/204
Use After Free	22-Jul-20	9.3	Use after free in developer tools in Google Chrome prior to 84.0.4147.89 allowed a remote attacker who had convinced the user to use developer tools to potentially exploit heap corruption via a crafted HTML page. **CVE ID : CVE-2020-6518**	N/A	A-GOO-CHRO-190820/205
N/A	22-Jul-20	4.3	Policy bypass in CSP in Google Chrome prior to 84.0.4147.89 allowed a remote attacker to bypass content security policy via a crafted HTML page. **CVE ID : CVE-2020-6519**	N/A	A-GOO-CHRO-190820/206
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	22-Jul-20	9.3	Buffer overflow in Skia in Google Chrome prior to 84.0.4147.89 allowed a remote attacker to potentially exploit heap corruption via a crafted HTML page. **CVE ID : CVE-2020-6520**	N/A	A-GOO-CHRO-190820/207

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Information Exposure	22-Jul-20	4.3	Side-channel information leakage in autofill in Google Chrome prior to 84.0.4147.89 allowed a remote attacker to obtain potentially sensitive information from process memory via a crafted HTML page. **CVE ID : CVE-2020-6521**	N/A	A-GOO-CHRO-190820/208
N/A	22-Jul-20	6.8	Inappropriate implementation in external protocol handlers in Google Chrome prior to 84.0.4147.89 allowed a remote attacker to potentially perform a sandbox escape via a crafted HTML page. **CVE ID : CVE-2020-6522**	N/A	A-GOO-CHRO-190820/209
Out-of-bounds Write	22-Jul-20	9.3	Out of bounds write in Skia in Google Chrome prior to 84.0.4147.89 allowed a remote attacker to potentially exploit heap corruption via a crafted HTML page. **CVE ID : CVE-2020-6523**	N/A	A-GOO-CHRO-190820/210
Out-of-bounds Write	22-Jul-20	9.3	Heap buffer overflow in WebAudio in Google Chrome prior to 84.0.4147.89 allowed a remote attacker to potentially exploit heap corruption via a crafted HTML page. **CVE ID : CVE-2020-6524**	N/A	A-GOO-CHRO-190820/211
Out-of-bounds	22-Jul-20	6.8	Heap buffer overflow in Skia in Google Chrome	N/A	A-GOO-CHRO-

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Write			prior to 84.0.4147.89 allowed a remote attacker to potentially exploit heap corruption via a crafted HTML page. **CVE ID : CVE-2020-6525**		190820/212
N/A	22-Jul-20	4.3	Inappropriate implementation in iframe sandbox in Google Chrome prior to 84.0.4147.89 allowed a remote attacker to bypass navigation restrictions via a crafted HTML page. **CVE ID : CVE-2020-6526**	N/A	A-GOO-CHRO-190820/213
Incorrect Default Permissions	22-Jul-20	4.3	Insufficient policy enforcement in CSP in Google Chrome prior to 84.0.4147.89 allowed a remote attacker to bypass content security policy via a crafted HTML page. **CVE ID : CVE-2020-6527**	N/A	A-GOO-CHRO-190820/214
Incorrect Authorizatio n	22-Jul-20	4.3	Incorrect security UI in basic auth in Google Chrome on iOS prior to 84.0.4147.89 allowed a remote attacker to spoof the contents of the Omnibox (URL bar) via a crafted HTML page. **CVE ID : CVE-2020-6528**	N/A	A-GOO-CHRO-190820/215
Improper Input Validation	22-Jul-20	4.3	Inappropriate implementation in WebRTC in Google Chrome prior to 84.0.4147.89 allowed an attacker in a privileged network position to leak cross-	N/A	A-GOO-CHRO-190820/216

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			origin data via a crafted HTML page. **CVE ID : CVE-2020-6529**		
Improper Restriction of Operations within the Bounds of a Memory Buffer	22-Jul-20	6.8	Out of bounds memory access in developer tools in Google Chrome prior to 84.0.4147.89 allowed an attacker who convinced a user to install a malicious extension to potentially exploit heap corruption via a crafted Chrome Extension. **CVE ID : CVE-2020-6530**	N/A	A-GOO-CHRO-190820/217
Information Exposure Through Discrepancy	22-Jul-20	4.3	Side-channel information leakage in scroll to text in Google Chrome prior to 84.0.4147.89 allowed a remote attacker to leak cross-origin data via a crafted HTML page. **CVE ID : CVE-2020-6531**	N/A	A-GOO-CHRO-190820/218
Access of Resource Using Incompatible Type ('Type Confusion')	22-Jul-20	6.8	Type Confusion in V8 in Google Chrome prior to 84.0.4147.89 allowed a remote attacker to potentially exploit heap corruption via a crafted HTML page. **CVE ID : CVE-2020-6533**	N/A	A-GOO-CHRO-190820/219
Out-of-bounds Write	22-Jul-20	6.8	Heap buffer overflow in WebRTC in Google Chrome prior to 84.0.4147.89 allowed a remote attacker to potentially exploit heap corruption via a crafted HTML page. **CVE ID : CVE-2020-6534**	N/A	A-GOO-CHRO-190820/220

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Improper Input Validation	22-Jul-20	4.3	Insufficient data validation in WebUI in Google Chrome prior to 84.0.4147.89 allowed a remote attacker who had compromised the renderer process to inject scripts or HTML into a privileged page via a crafted HTML page. **CVE ID : CVE-2020-6535**	N/A	A-GOO-CHRO-190820/221
N/A	22-Jul-20	4.3	Incorrect security UI in PWAs in Google Chrome prior to 84.0.4147.89 allowed a remote attacker who had persuaded the user to install a PWA to spoof the contents of the Omnibox (URL bar) via a crafted PWA. **CVE ID : CVE-2020-6536**	N/A	A-GOO-CHRO-190820/222
grafana					
grafana					
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	27-Jul-20	4.3	Grafana through 6.7.1 allows stored XSS due to insufficient input protection in the originalUrl field, which allows an attacker to inject JavaScript code that will be executed after clicking on Open Original Dashboard after visiting the snapshot. **CVE ID : CVE-2020-11110**	https://security.netapp.com/advisory/ntap-20200810-0002/	A-GRA-GRAF-190820/223
graylog					
graylog					
Improper Certificate	17-Jul-20	6.8	Graylog before 3.3.3 lacks SSL Certificate Validation	N/A	A-GRA-GRAY-190820/224

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Validation			for LDAP servers. It allows use of an external user/group database stored in LDAP. The connection configuration allows the usage of unencrypted, SSL- or TLS-secured connections. Unfortunately, the Graylog client code (in all versions that support LDAP) does not implement proper certificate validation (regardless of whether the "Allow self-signed certificates" option is used). Therefore, any attacker with the ability to intercept network traffic between a Graylog server and an LDAP server is able to redirect traffic to a different LDAP server (unnoticed by the Graylog server due to the lack of certificate validation), effectively bypassing Graylog's authentication mechanism. **CVE ID : CVE-2020-15813**		
grin					
grin					
Insufficient Verification of Data Authenticity	28-Jul-20	5	Grin 3.0.0 before 4.0.0 has insufficient validation of data related to Mimblewimble. **CVE ID : CVE-2020-15899**	https://github.com/mimblewimble/grin-security/blob/master/CVEs/CVE-2020-	A-GRI-GRIN-190820/225

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
				15899.md	
grundfos					
cim_500					
Insufficiently Protected Credentials	27-Jul-20	5	Grundfos CIM 500 v06.16.00 stores plaintext credentials, which may allow sensitive information to be read or allow modification to system settings by someone with access to the device. **CVE ID : CVE-2020-10609**	https://us-cert.cisa.gov/ics/advisories/icsa-20-189-01	A-GRU-CIM_-190820/226
hashicorp					
terraform_enterprise					
Improper Input Validation	30-Jul-20	5	HashiCorp Terraform Enterprise up to v202006-1 contained a default signup page that allowed user registration even when disabled, bypassing SAML enforcement. Fixed in v202007-1. **CVE ID : CVE-2020-15511**	N/A	A-HAS-TERR-190820/227
hcltech					
bigfix_platform					
Insufficiently Protected Credentials	16-Jul-20	2.1	"BigFix Platform is storing clear text credentials within the system's memory. An attacker who is able to gain administrative privileges can use a program to create a memory dump and extract the credentials. These credentials can be used to pivot further into the environment. The	N/A	A-HCL-BIGF-190820/228

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			principle of least privilege should be applied to all BigFix deployments, limiting administrative access." **CVE ID : CVE-2020-4095**		
bigfix_webui					
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	17-Jul-20	3.5	HCL BigFix WebUI is vulnerable to stored cross-site scripting (XSS) within the Apps->Software module. An attacker can use XSS to send a malicious script to an unsuspecting user. This affects all versions prior to latest releases as specified in https://support.hcltechsw.com/csm?id=kb_article&sysparm_article=KB0080855&sys_kb_id=971d99ed1b8ed01c086dcbfc0a4bcb6a. **CVE ID : CVE-2020-4104**	https://support.hcltechsw.com/csm?id=kb_article&sysparm_article=KB0080855	A-HCL-BIGF-190820/229
hmtalk					
daviewindy					
Out-of-bounds Write	17-Jul-20	6.8	DaviewIndy 8.98.9 and earlier has a Heap-based overflow vulnerability, triggered when the user opens a malformed PDF file that is mishandled by Daview.exe. Attackers could exploit this and arbitrary code execution. **CVE ID : CVE-2020-7818**	https://www.krcert.or.kr/krcert/secNoticeView.do?bulletin_writing_sequence=35521	A-HMT-DAVI-190820/230
Use After Free	30-Jul-20	6.8	DaviewIndy 8.98.7 and earlier version contain	N/A	A-HMT-DAVI-190820/231

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Use-After-Free vulnerability, triggered when the user opens a malformed specific file that is mishandled by Daview.exe. Attackers could exploit this and arbitrary code execution. **CVE ID : CVE-2020-7827**		
Out-of-bounds Write	30-Jul-20	6.8	DaviewIndy 8.98.4 and earlier version contain Heap-based overflow vulnerability, triggered when the user opens a malformed specific file that is mishandled by Daview.exe. Attackers could exploit this and arbitrary code execution. **CVE ID : CVE-2020-7828**	N/A	A-HMT-DAVI-190820/232
Out-of-bounds Write	30-Jul-20	6.8	DaviewIndy 8.98.4 and earlier version contain Heap-based overflow vulnerability, triggered when the user opens a malformed specific file that is mishandled by Daview.exe. Attackers could exploit this and arbitrary code execution. **CVE ID : CVE-2020-7829**	N/A	A-HMT-DAVI-190820/233
HP					
nagios-plugins-hpilo					
Improper Control of Generation of Code ('Code	17-Jul-20	7.5	HP nagios plugin for iLO (nagios-plugins-hpilo v1.50 and earlier) has a php code injection vulnerability.	https://github.com/HewlettPackard/nagios-plugins-hpilo/commit/7617b273	A-HP-NAGI-190820/234

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Injection')			**CVE ID : CVE-2020-7206**	6a95c7f354198f092febe37e7005c677	
hpe					
intelligent_provisioning					
Improper Control of Generation of Code ('Code Injection')	30-Jul-20	7.2	A potential security vulnerability has been identified in HPE Intelligent Provisioning, Service Pack for ProLiant, and HPE Scripting ToolKit. The vulnerability could be locally exploited to allow arbitrary code execution during the boot process. **Note:** This vulnerability is related to using insmod in GRUB2 in the specific impacted HPE product and HPE is addressing this issue. HPE has made the following software updates and mitigation information to resolve the vulnerability in Intelligent Provisioning, Service Pack for ProLiant, and HPE Scripting ToolKit. HPE provided latest Intelligent Provisioning, Service Pack for ProLiant, and HPE Scripting Toolkit which includes the GRUB2 patch to resolve this vulnerability. These new boot images will update GRUB2 and the Forbidden Signature Database (DBX). After the DBX is updated, users will not be able to	N/A	A-HPE-INTE-190820/235

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			boot to the older IP, SPP or Scripting ToolKit with Secure Boot enabled. HPE have provided a standalone DBX update tool to work with Microsoft Windows, and supported Linux Operating Systems. These tools can be used to update the Forbidden Signature Database (DBX) from within the OS. **Note:** This DBX update mitigates the GRUB2 issue with insmod enabled, and the "Boot Hole" issue for HPE signed GRUB2 applications. **CVE ID : CVE-2020-7205**		
service_pack_for_proliant					
Improper Control of Generation of Code ('Code Injection')	30-Jul-20	7.2	A potential security vulnerability has been identified in HPE Intelligent Provisioning, Service Pack for ProLiant, and HPE Scripting ToolKit. The vulnerability could be locally exploited to allow arbitrary code execution during the boot process. **Note:** This vulnerability is related to using insmod in GRUB2 in the specific impacted HPE product and HPE is addressing this issue. HPE has made the following software updates and mitigation information to	N/A	A-HPE-SERV-190820/236

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			resolve the vulnerability in Intelligent Provisioning, Service Pack for ProLiant, and HPE Scripting ToolKit. HPE provided latest Intelligent Provisioning, Service Pack for ProLiant, and HPE Scripting Toolkit which includes the GRUB2 patch to resolve this vulnerability. These new boot images will update GRUB2 and the Forbidden Signature Database (DBX). After the DBX is updated, users will not be able to boot to the older IP, SPP or Scripting ToolKit with Secure Boot enabled. HPE have provided a standalone DBX update tool to work with Microsoft Windows, and supported Linux Operating Systems. These tools can be used to update the Forbidden Signature Database (DBX) from within the OS. **Note:** This DBX update mitigates the GRUB2 issue with insmod enabled, and the "Boot Hole" issue for HPE signed GRUB2 applications. **CVE ID : CVE-2020-7205**		
smartstart_scripting_toolkit					
Improper Control of Generation	30-Jul-20	7.2	A potential security vulnerability has been identified in HPE	N/A	A-HPE-SMAR-190820/237

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
of Code ('Code Injection')			Intelligent Provisioning, Service Pack for ProLiant, and HPE Scripting ToolKit. The vulnerability could be locally exploited to allow arbitrary code execution during the boot process. **Note:** This vulnerability is related to using insmod in GRUB2 in the specific impacted HPE product and HPE is addressing this issue. HPE has made the following software updates and mitigation information to resolve the vulnerability in Intelligent Provisioning, Service Pack for ProLiant, and HPE Scripting ToolKit. HPE provided latest Intelligent Provisioning, Service Pack for ProLiant, and HPE Scripting Toolkit which includes the GRUB2 patch to resolve this vulnerability. These new boot images will update GRUB2 and the Forbidden Signature Database (DBX). After the DBX is updated, users will not be able to boot to the older IP, SPP or Scripting ToolKit with Secure Boot enabled. HPE have provided a standalone DBX update tool to work with Microsoft Windows, and supported Linux Operating Systems. These tools can		

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			be used to update the Forbidden Signature Database (DBX) from within the OS. **Note:** This DBX update mitigates the GRUB2 issue with insmod enabled, and the "Boot Hole" issue for HPE signed GRUB2 applications. **CVE ID : CVE-2020-7205**		
Huawei					
fusioncompute					
Incorrect Authorization	31-Jul-20	4.6	Huawei FusionComput 8.0.0 have an improper authorization vulnerability. A module does not verify some input correctly and authorizes files with incorrect access. Attackers can exploit this vulnerability to launch privilege escalation attack. This can compromise normal service. **CVE ID : CVE-2020-9248**	N/A	A-HUA-FUSI-190820/238
IBM					
planning_analytics_local					
Improper Input Validation	29-Jul-20	5.8	IBM Planning Analytics Local 2.0.0 through 2.0.9.1 could allow a remote attacker to hijack the clicking action of the victim. By persuading a victim to visit a malicious Web site, a remote attacker could exploit this vulnerability to hijack the victim's click actions and	https://www.ibm.com/support/pages/node/6253355	A-IBM-PLAN-190820/239

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			possibly launch further attacks against the victim. IBM X-Force ID: 185716. **CVE ID : CVE-2020-4644**		
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	29-Jul-20	3.5	IBM Planning Analytics Local 2.0.0 through 2.0.9.1 is vulnerable to cross-site scripting. This vulnerability allows users to embed arbitrary JavaScript code in the Web UI thus altering the intended functionality potentially leading to credentials disclosure within a trusted session. IBM X-Force ID: 185717. **CVE ID : CVE-2020-4645**	https://www.ibm.com/support/pages/node/6253355	A-IBM-PLAN-190820/240
mq_for_hpe_nonstop					
N/A	20-Jul-20	4	IBM MQ for HPE NonStop 8.0.4 and 8.1.0 could allow a remote authenticated attacker could cause a denial of service due to an error within the Queue processing function. IBM X-Force ID: 181563. **CVE ID : CVE-2020-4466**	https://www.ibm.com/support/pages/node/6250473	A-IBM-MQ_F-190820/241
mq_appliance					
Information Exposure	28-Jul-20	3.5	IBM MQ, IBM MQ Appliance, and IBM MQ for HPE NonStop 8.0, 9.1 LTS, and 9.1 CD could allow under special circumstances, an authenticated user to obtain sensitive information due to a data leak from an error	https://www.ibm.com/support/pages/node/6252777	A-IBM-MQ_A-190820/242

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			message within the pre-v7 pubsub logic. IBM X-Force ID: 177402. **CVE ID : CVE-2020-4319**		
Missing Release of Resource after Effective Lifetime	28-Jul-20	5	IBM MQ, IBM MQ Appliance, IBM MQ for HPE NonStop 8.0, 9.1 CD, and 9.1 LTS could allow an attacker to cause a denial of service due to a memory leak caused by an error creating a dynamic queue. IBM X-Force ID: 179080. **CVE ID : CVE-2020-4375**	https://www.ibm.com/support/pages/node/6252785	A-IBM-MQ_A-190820/243
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	28-Jul-20	4	IBM MQ, IBM MQ Appliance, and IBM MQ for HPE NonStop 8.0, 9.1 CD, and 9.1 LTS is vulnerable to a buffer overflow vulnerability due to an error within the channel processing code. A remote attacker could overflow the buffer using an older client and cause a denial of service. IBM X-Force ID: 181562. **CVE ID : CVE-2020-4465**	https://www.ibm.com/support/pages/node/6252783	A-IBM-MQ_A-190820/244
Information Exposure	27-Jul-20	2.1	IBM MQ Appliance 9.1 LTS and 9.1 CD could allow a local privileged user to obtain highly sensitve information due to inclusion of data within trace files. IBM X-Force ID: 182118. **CVE ID : CVE-2020-4498**	https://www.ibm.com/support/pages/node/6252409	A-IBM-MQ_A-190820/245
planning_analytics					

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Information Exposure	20-Jul-20	4	IBM Planning Analytics 2.0 could allow a remote attacker to obtain sensitive information by disclosing private IP addresses in HTTP responses. IBM X-Force ID: 178766. **CVE ID : CVE-2020-4361**	https://www.ibm.com/support/pages/node/6249981	A-IBM-PLAN-190820/246
Session Fixation	20-Jul-20	4.3	IBM Planning Analytics 2.0 could allow a remote attacker to obtain sensitive information, caused by the failure to set the Secure flag for the session cookie in TLS mode. By intercepting its transmission within an HTTP session, an attacker could exploit this vulnerability to capture the cookie and obtain sensitive information. IBM X-Force ID: 182631. **CVE ID : CVE-2020-4527**	https://www.ibm.com/support/pages/node/6249981	A-IBM-PLAN-190820/247
security_guardium					
Use of a Broken or Risky Cryptographic Algorithm	30-Jul-20	5	IBM Security Guardium 10.5, 10.6, and 11.1 uses weaker than expected cryptographic algorithms that could allow an attacker to decrypt highly sensitive information. IBM X-Force ID: 174803. **CVE ID : CVE-2020-4185**	https://www.ibm.com/support/pages/node/6254369	A-IBM-SECU-190820/248
Information Exposure	30-Jul-20	5	IBM Security Guardium 10.5, 10.6, and 11.1 could disclose sensitive information on the login page that could aid in	https://www.ibm.com/support/pages/node/6254367	A-IBM-SECU-190820/249

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			further attacks against the system. IBM X-Force ID: 174804. **CVE ID : CVE-2020-4186**		
security_key_lifecycle_manager					
Insufficiently Protected Credentials	29-Jul-20	5	IBM Tivoli Key Lifecycle Manager 3.0.1 and 4.0 uses an inadequate account lockout setting that could allow a remote attacker to brute force account credentials. IBM X-Force ID: 184156. **CVE ID : CVE-2020-4567**	https://www.ibm.com/support/pages/node/6253781	A-IBM-SECU-190820/250
Exposure of Resource to Wrong Sphere	29-Jul-20	6.4	IBM Tivoli Key Lifecycle Manager 3.0.1 and 4.0 uses a protection mechanism that relies on the existence or values of an input, but the input can be modified by an untrusted actor in a way that bypasses the protection mechanism. IBM X-Force ID: 184158. **CVE ID : CVE-2020-4569**	https://www.ibm.com/support/pages/node/6253781	A-IBM-SECU-190820/251
Information Exposure	29-Jul-20	5	IBM Tivoli Key Lifecycle Manager 3.0.1 and 4.0 could allow a remote attacker to obtain sensitive information when a detailed technical error message is returned in the browser. This information could be used in further attacks against the system. IBM X-Force ID: 184179. **CVE ID : CVE-2020-4572**	https://www.ibm.com/support/pages/node/6253781	A-IBM-SECU-190820/252
Information	29-Jul-20	5	IBM Tivoli Key Lifecycle	https://ww	A-IBM-SECU-

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Exposure			Manager 3.0.1 and 4.0 could disclose sensitive information due to responding to unauthenticated HTTP requests. IBM X-Force ID: 184180. **CVE ID : CVE-2020-4573**	w.ibm.com/support/pages/node/6253781	190820/253
Weak Password Requirements	29-Jul-20	5	IBM Tivoli Key Lifecycle Manager does not require that users should have strong passwords by default, which makes it easier for attackers to compromise user accounts. IBM X-Force ID: 184181. **CVE ID : CVE-2020-4574**	https://www.ibm.com/support/pages/node/6253781	A-IBM-SECU-190820/254
filenet_content_manager					
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	23-Jul-20	3.5	IBM FileNet Content Manager 5.5.3 and 5.5.4 is vulnerable to cross-site scripting. This vulnerability allows users to embed arbitrary JavaScript code in the Web UI thus altering the intended functionality potentially leading to credentials disclosure within a trusted session. IBM X-Force ID: 181227. **CVE ID : CVE-2020-4447**	https://www.ibm.com/support/pages/node/6208453	A-IBM-FILE-190820/255
websphere_application_server					
Deserialization of Untrusted Data	17-Jul-20	9	IBM WebSphere Application Server 7.0, 8.0, 8.5, and 9.0 traditional could allow a remote attacker to execute	https://www.ibm.com/support/pages/node/6250	A-IBM-WEBS-190820/256

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			arbitrary code on a system with a specially-crafted sequence of serialized objects over the SOAP connector. IBM X-Force ID: 181489. **CVE ID : CVE-2020-4464**	059	
maximo_asset_management					
Improper Restriction of XML External Entity Reference ('XXE')	29-Jul-20	6.4	IBM Maximo Asset Management 7.6.0.1 and 7.6.0.2 is vulnerable to an XML External Entity Injection (XXE) attack when processing XML data. A remote attacker could exploit this vulnerability to expose sensitive information or consume memory resources. IBM X-Force ID: 181484. **CVE ID : CVE-2020-4463**	https://www.ibm.com/support/pages/node/6253953	A-IBM-MAXI-190820/257
intelligent_operations_center					
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	28-Jul-20	3.5	IBM Intelligent Operations Center for Emergency Management, Intelligent Operations Center (IOC), and IBM Water Operations for Waternamics are vulnerable to cross-site scripting. This vulnerability allows users to embed arbitrary JavaScript code in the Web UI thus altering the intended functionality potentially leading to credentials disclosure within a trusted session.	https://www.ibm.com/support/pages/node/6253295	A-IBM-INTE-190820/258

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			IBM X-Force ID: 177355. **CVE ID : CVE-2020-4317**		
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	28-Jul-20	3.5	IBM Intelligent Operations Center for Emergency Management, Intelligent Operations Center (IOC), and IBM Water Operations for Waternamics are vulnerable to cross-site scripting. This vulnerability allows users to embed arbitrary JavaScript code in the Web UI thus altering the intended functionality potentially leading to credentials disclosure within a trusted session. IBM X-Force ID: 177356. **CVE ID : CVE-2020-4318**	https://www.ibm.com/support/pages/node/6253297	A-IBM-INTE-190820/259
intelligent_operations_center_for_emergency_management					
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	28-Jul-20	3.5	IBM Intelligent Operations Center for Emergency Management, Intelligent Operations Center (IOC), and IBM Water Operations for Waternamics are vulnerable to cross-site scripting. This vulnerability allows users to embed arbitrary JavaScript code in the Web UI thus altering the intended functionality potentially leading to credentials disclosure within a trusted session. IBM X-Force ID: 177355. **CVE ID : CVE-2020-4317**	https://www.ibm.com/support/pages/node/6253295	A-IBM-INTE-190820/260

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	28-Jul-20	3.5	IBM Intelligent Operations Center for Emergency Management, Intelligent Operations Center (IOC), and IBM Water Operations for Waternamics are vulnerable to cross-site scripting. This vulnerability allows users to embed arbitrary JavaScript code in the Web UI thus altering the intended functionality potentially leading to credentials disclosure within a trusted session. IBM X-Force ID: 177356. **CVE ID : CVE-2020-4318**	https://www.ibm.com/support/pages/node/6253297	A-IBM-INTE-190820/261
water_operations_for_waternamics					
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	28-Jul-20	3.5	IBM Intelligent Operations Center for Emergency Management, Intelligent Operations Center (IOC), and IBM Water Operations for Waternamics are vulnerable to cross-site scripting. This vulnerability allows users to embed arbitrary JavaScript code in the Web UI thus altering the intended functionality potentially leading to credentials disclosure within a trusted session. IBM X-Force ID: 177355. **CVE ID : CVE-2020-4317**	https://www.ibm.com/support/pages/node/6253295	A-IBM-WATE-190820/262
Improper Neutralization of Input	28-Jul-20	3.5	IBM Intelligent Operations Center for Emergency Management, Intelligent	https://www.ibm.com/support/page	A-IBM-WATE-190820/263

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
During Web Page Generation ('Cross-site Scripting')			Operations Center (IOC), and IBM Water Operations for Waternamics are vulnerable to cross-site scripting. This vulnerability allows users to embed arbitrary JavaScript code in the Web UI thus altering the intended functionality potentially leading to credentials disclosure within a trusted session. IBM X-Force ID: 177356. **CVE ID : CVE-2020-4318**	s/node/6253297	
marketing_operations					
Download of Code Without Integrity Check	20-Jul-20	5.5	Using HCL Marketing Operations 9.1.2.4, 10.1.x, 11.1.0.x, a malicious attacker could download files from the RHEL environment by doing some modification in the link, giving the attacker access to confidential information. **CVE ID : CVE-2020-4125**	N/A	A-IBM-MARK-190820/264
publishing_engine					
N/A	16-Jul-20	4.3	IBM Publishing Engine 6.0.6, 6.0.6.1, and 7.0 does not set the secure attribute on authorization tokens or session cookies. Attackers may be able to get the cookie values by sending a http:// link to a user or by planting this link in a site the user goes to. The cookie will be sent to the	https://www.ibm.com/support/pages/node/6249131	A-IBM-PUBL-190820/265

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			insecure link and the attacker can then obtain the cookie value by snooping the traffic. IBM X-Force ID: 177354. **CVE ID : CVE-2020-4316**		
rational_publishing_engine					
N/A	16-Jul-20	4.3	IBM Publishing Engine 6.0.6, 6.0.6.1, and 7.0 does not set the secure attribute on authorization tokens or session cookies. Attackers may be able to get the cookie values by sending a http:// link to a user or by planting this link in a site the user goes to. The cookie will be sent to the insecure link and the attacker can then obtain the cookie value by snooping the traffic. IBM X-Force ID: 177354. **CVE ID : CVE-2020-4316**	https://www.ibm.com/support/pages/node/6249131	A-IBM-RATI-190820/266
verify_gateway					
Cleartext Storage of Sensitive Information	22-Jul-20	2.1	IBM Verify Gateway (IVG) 1.0.0 and 1.0.1 stores highly sensitive information in cleartext that could be obtained by a user. IBM X-Force ID: 179004. **CVE ID : CVE-2020-4369**	https://www.ibm.com/support/pages/node/6251285	A-IBM-VERI-190820/267
Insecure Storage of Sensitive Information	22-Jul-20	2.1	IBM Verify Gateway (IVG) 1.0.0 and 1.0.1 contains sensitive information in leftover debug code that could be used aid a local user in further attacks	https://www.ibm.com/support/pages/node/6251287	A-IBM-VERI-190820/268

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			against the system. IBM X-Force ID: 179008. **CVE ID : CVE-2020-4371**		
Insufficiently Protected Credentials	22-Jul-20	2.1	IBM Verify Gateway (IVG) 1.0.0 and 1.0.1 stores user credentials in plain in clear text which can be read by a local user. IBM X-Force ID: 179009 **CVE ID : CVE-2020-4372**	https://www.ibm.com/support/pages/node/6251289	A-IBM-VERI-190820/269
Use of Hard-coded Credentials	22-Jul-20	7.5	IBM Verify Gateway (IVG) 1.0.0 and 1.0.1 contains hard-coded credentials, such as a password or cryptographic key, which it uses for its own inbound authentication, outbound communication to external components, or encryption of internal data. IBM X-Force ID: 179266. **CVE ID : CVE-2020-4385**	https://www.ibm.com/support/pages/node/6251291	A-IBM-VERI-190820/270
Cleartext Transmission of Sensitive Information	22-Jul-20	4.3	IBM Verify Gateway (IVG) 1.0.0 and 1.0.1 transmits sensitive information in plain text which could be obtained by an attacker using man in the middle techniques. IBM X-Force ID: 179428. **CVE ID : CVE-2020-4397**	https://www.ibm.com/support/pages/node/6251321	A-IBM-VERI-190820/271
N/A	22-Jul-20	4	IBM Verify Gateway (IVG) 1.0.0 and 1.0.1 could allow an authenticated user to send malformed requests to cause a denial of service against the server. IBM X-Force ID: 179476.	https://www.ibm.com/support/pages/node/6251323	A-IBM-VERI-190820/272

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2020-4399		
Insufficiently Protected Credentials	22-Jul-20	5	IBM Verify Gateway (IVG) 1.0.0 and 1.0.1 uses an inadequate account lockout setting that could allow a remote attacker to brute force account credentials. IBM X-Force ID: 179478. **CVE ID : CVE-2020-4400**	https://www.ibm.com/support/pages/node/6251279	A-IBM-VERI-190820/273
Information Exposure Through Log Files	27-Jul-20	4	IBM Verify Gateway (IVG) 1.0.0 and 1.0.1 could disclose potentially sensitive information to an authenticated user due to world readable log files. IBM X-Force ID: 179484. **CVE ID : CVE-2020-4405**	https://www.ibm.com/support/pages/node/6252479	A-IBM-VERI-190820/274
qradar_advisory					
Insufficiently Protected Credentials	27-Jul-20	2.1	The IBM QRadar Advisor 1.1 through 2.5.2 with Watson App for IBM QRadar SIEM does not adequately mask all passwords during input, which could be obtained by a physical attacker nearby. IBM X-Force ID: 179536. **CVE ID : CVE-2020-4408**	https://www.ibm.com/support/pages/node/6252401	A-IBM-QRAD-190820/275
sterling_external_authentication_server					
Improper Restriction of XML External Entity Reference ('XXE')	16-Jul-20	6.4	IBM Sterling External Authentication Server 6.0.1, 6.0.0, 2.4.3.2, and 2.4.2 and IBM Sterling Secure Proxy 6.0.1, 6.0.0, 3.4.3, and 3.4.2 are vulnerable to an XML	https://www.ibm.com/support/pages/node/6249317, https://www.ibm.com/s	A-IBM-STER-190820/276

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			External Entity Injection (XXE) attack when processing XML data. A remote attacker could exploit this vulnerability to expose sensitive information or consume memory resources. IBM X-Force ID: 181482. **CVE ID : CVE-2020-4462**	upport/pages/node/6249331	
sterling_secure_proxy					
Improper Restriction of XML External Entity Reference ('XXE')	16-Jul-20	6.4	IBM Sterling External Authentication Server 6.0.1, 6.0.0, 2.4.3.2, and 2.4.2 and IBM Sterling Secure Proxy 6.0.1, 6.0.0, 3.4.3, and 3.4.2 are vulnerable to an XML External Entity Injection (XXE) attack when processing XML data. A remote attacker could exploit this vulnerability to expose sensitive information or consume memory resources. IBM X-Force ID: 181482. **CVE ID : CVE-2020-4462**	https://www.ibm.com/support/pages/node/6249317, https://www.ibm.com/support/pages/node/6249331	A-IBM-STER-190820/277
icegram					
email_subscribers_\&_newsletters					
Cross-Site Request Forgery (CSRF)	17-Jul-20	4.3	Cross-site request forgery in Icegram Email Subscribers & Newsletters Plugin for WordPress v4.4.8 allows a remote attacker to send forged emails by tricking legitimate users into clicking a crafted link.	https://www.tenable.com/security/research/tra-2020-44-0	A-ICE-EMAI-190820/278

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2020-5767		
Improper Neutralization of Special Elements used in an SQL Command ('SQL Injection')	17-Jul-20	4	Improper Neutralization of Special Elements used in an SQL Command ('SQL Injection') in Icegram Email Subscribers & Newsletters Plugin for WordPress v4.4.8 allows a remote, authenticated attacker to determine the value of database fields. **CVE ID : CVE-2020-5768**	https://www.tenable.com/security/research/tra-2020-44-0	A-ICE-EMAI-190820/279
Iconics					
energy_analytix					
Deserialization of Untrusted Data	16-Jul-20	7.5	A specially crafted communication packet sent to the affected devices could allow remote code execution and a denial-of-service condition due to a deserialization vulnerability. This issue affects: Mitsubishi Electric MC Works64 version 4.02C (10.95.208.31) and earlier, all versions; Mitsubishi Electric MC Works32 version 3.00A (9.50.255.02); ICONICS GenBroker64, Platform Services, Workbench, FrameWorX Server version 10.96 and prior; ICONICS GenBroker32 version 9.5 and prior. **CVE ID : CVE-2020-12007**	https://us-cert.cisa.gov/ics/advisories/icsa-20-170-02,, https://us-cert.cisa.gov/ics/advisories/icsa-20-170-03	A-ICO-ENER-190820/280
Deserialization of Untrusted	16-Jul-20	5	A specially crafted communication packet sent to the affected device	https://us-cert.cisa.gov/ics/advisorie	A-ICO-ENER-190820/281

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Data			could cause a denial-of-service condition due to a deserialization vulnerability. This affects: Mitsubishi Electric MC Works64 Version 4.02C (10.95.208.31) and earlier, all versions; Mitsubishi Electric MC Works32 Version 3.00A (9.50.255.02); ICONICS GenBroker64, Platform Services, Workbench, FrameWorX Server v10.96 and prior; ICONICS GenBroker32 v9.5 and prior. **CVE ID : CVE-2020-12009**	s/icsa-20-170-02, https://us-cert.cisa.gov/ics/advisories/icsa-20-170-03	
Out-of-bounds Write	16-Jul-20	7.5	A specially crafted communication packet sent to the affected systems could cause a denial-of-service condition or allow remote code execution. This issue affects: Mitsubishi Electric MC Works64 version 4.02C (10.95.208.31) and earlier, all versions; MC Works32 version 3.00A (9.50.255.02); ICONICS GenBroker64, Platform Services, Workbench, FrameWorX Server version 10.96 and prior; GenBroker32 version 9.5 and prior. **CVE ID : CVE-2020-12011**	N/A	A-ICO-ENER-190820/282
Improper Control of	16-Jul-20	6.4	A specially crafted WCF client that interfaces to the	https://us-cert.cisa.gov/	A-ICO-ENER-190820/283

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Generation of Code ('Code Injection')			may allow the execution of certain arbitrary SQL commands remotely. This affects: Mitsubishi Electric MC Works64 Version 4.02C (10.95.208.31) and earlier, all versions; Mitsubishi Electric MC Works32 Version 3.00A (9.50.255.02); ICONICS GenBroker64, Platform Services, Workbench, FrameWorX Server v10.96 and prior; ICONICS GenBroker32 v9.5 and prior. **CVE ID : CVE-2020-12013**	ics/advisories/icsa-20-170-02, https://us-cert.cisa.gov/ics/advisories/icsa-20-170-03	
Deserialization of Untrusted Data	16-Jul-20	5	A specially crafted communication packet sent to the affected systems could cause a denial-of-service condition due to improper deserialization. This issue affects: Mitsubishi Electric MC Works64 version 4.02C (10.95.208.31) and earlier, all versions; Mitsubishi Electric MC Works32 version 3.00A (9.50.255.02); ICONICS GenBroker64, Platform Services, Workbench, FrameWorX Server version 10.96 and prior; ICONICS GenBroker32 version 9.5 and prior. **CVE ID : CVE-2020-12015**	https://www.us-cert.gov/ics/advisories/icsa-20-170-02, https://www.us-cert.gov/ics/advisories/icsa-20-170-03	A-ICO-ENER-190820/284
facility_analytix					

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Deserialization of Untrusted Data	16-Jul-20	7.5	A specially crafted communication packet sent to the affected devices could allow remote code execution and a denial-of-service condition due to a deserialization vulnerability. This issue affects: Mitsubishi Electric MC Works64 version 4.02C (10.95.208.31) and earlier, all versions; Mitsubishi Electric MC Works32 version 3.00A (9.50.255.02); ICONICS GenBroker64, Platform Services, Workbench, FrameWorX Server version 10.96 and prior; ICONICS GenBroker32 version 9.5 and prior. **CVE ID : CVE-2020-12007**	https://us-cert.cisa.gov/ics/advisories/icsa-20-170-02,, https://us-cert.cisa.gov/ics/advisories/icsa-20-170-03	A-ICO-FACI-190820/285
Deserialization of Untrusted Data	16-Jul-20	5	A specially crafted communication packet sent to the affected device could cause a denial-of-service condition due to a deserialization vulnerability. This affects: Mitsubishi Electric MC Works64 Version 4.02C (10.95.208.31) and earlier, all versions; Mitsubishi Electric MC Works32 Version 3.00A (9.50.255.02); ICONICS GenBroker64, Platform Services, Workbench, FrameWorX Server v10.96 and prior; ICONICS GenBroker32 v9.5 and	https://us-cert.cisa.gov/ics/advisories/icsa-20-170-02, https://us-cert.cisa.gov/ics/advisories/icsa-20-170-03	A-ICO-FACI-190820/286

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			prior. **CVE ID : CVE-2020-12009**		
Out-of-bounds Write	16-Jul-20	7.5	A specially crafted communication packet sent to the affected systems could cause a denial-of-service condition or allow remote code execution. This issue affects: Mitsubishi Electric MC Works64 version 4.02C (10.95.208.31) and earlier, all versions; MC Works32 version 3.00A (9.50.255.02); ICONICS GenBroker64, Platform Services, Workbench, FrameWorX Server version 10.96 and prior; GenBroker32 version 9.5 and prior. **CVE ID : CVE-2020-12011**	N/A	A-ICO-FACI-190820/287
Improper Control of Generation of Code ('Code Injection')	16-Jul-20	6.4	A specially crafted WCF client that interfaces to the may allow the execution of certain arbitrary SQL commands remotely. This affects: Mitsubishi Electric MC Works64 Version 4.02C (10.95.208.31) and earlier, all versions; Mitsubishi Electric MC Works32 Version 3.00A (9.50.255.02); ICONICS GenBroker64, Platform Services, Workbench, FrameWorX Server v10.96 and prior; ICONICS GenBroker32 v9.5 and prior.	https://us-cert.cisa.gov/ics/advisories/icsa-20-170-02, https://us-cert.cisa.gov/ics/advisories/icsa-20-170-03	A-ICO-FACI-190820/288

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2020-12013		
Deserialization of Untrusted Data	16-Jul-20	5	A specially crafted communication packet sent to the affected systems could cause a denial-of-service condition due to improper deserialization. This issue affects: Mitsubishi Electric MC Works64 version 4.02C (10.95.208.31) and earlier, all versions; Mitsubishi Electric MC Works32 version 3.00A (9.50.255.02); ICONICS GenBroker64, Platform Services, Workbench, FrameWorX Server version 10.96 and prior; ICONICS GenBroker32 version 9.5 and prior. **CVE ID : CVE-2020-12015**	https://www.us-cert.gov/ics/advisories/icsa-20-170-02, https://www.us-cert.gov/ics/advisories/icsa-20-170-03	A-ICO-FACI-190820/289
genesis64					
Deserialization of Untrusted Data	16-Jul-20	7.5	A specially crafted communication packet sent to the affected devices could allow remote code execution and a denial-of-service condition due to a deserialization vulnerability. This issue affects: Mitsubishi Electric MC Works64 version 4.02C (10.95.208.31) and earlier, all versions; Mitsubishi Electric MC Works32 version 3.00A (9.50.255.02); ICONICS GenBroker64, Platform Services, Workbench,	https://us-cert.cisa.gov/ics/advisories/icsa-20-170-02,, https://us-cert.cisa.gov/ics/advisories/icsa-20-170-03	A-ICO-GENE-190820/290

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			FrameWorX Server version 10.96 and prior; ICONICS GenBroker32 version 9.5 and prior. **CVE ID : CVE-2020-12007**		
Deserialization of Untrusted Data	16-Jul-20	5	A specially crafted communication packet sent to the affected device could cause a denial-of-service condition due to a deserialization vulnerability. This affects: Mitsubishi Electric MC Works64 Version 4.02C (10.95.208.31) and earlier, all versions; Mitsubishi Electric MC Works32 Version 3.00A (9.50.255.02); ICONICS GenBroker64, Platform Services, Workbench, FrameWorX Server v10.96 and prior; ICONICS GenBroker32 v9.5 and prior. **CVE ID : CVE-2020-12009**	https://us-cert.cisa.gov/ics/advisories/icsa-20-170-02, https://us-cert.cisa.gov/ics/advisories/icsa-20-170-03	A-ICO-GENE-190820/291
Out-of-bounds Write	16-Jul-20	7.5	A specially crafted communication packet sent to the affected systems could cause a denial-of-service condition or allow remote code execution. This issue affects: Mitsubishi Electric MC Works64 version 4.02C (10.95.208.31) and earlier, all versions; MC Works32 version 3.00A (9.50.255.02); ICONICS GenBroker64, Platform	N/A	A-ICO-GENE-190820/292

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Services, Workbench, FrameWorX Server version 10.96 and prior; GenBroker32 version 9.5 and prior. **CVE ID : CVE-2020-12011**		
Improper Control of Generation of Code ('Code Injection')	16-Jul-20	6.4	A specially crafted WCF client that interfaces to the may allow the execution of certain arbitrary SQL commands remotely. This affects: Mitsubishi Electric MC Works64 Version 4.02C (10.95.208.31) and earlier, all versions; Mitsubishi Electric MC Works32 Version 3.00A (9.50.255.02); ICONICS GenBroker64, Platform Services, Workbench, FrameWorX Server v10.96 and prior; ICONICS GenBroker32 v9.5 and prior. **CVE ID : CVE-2020-12013**	https://us-cert.cisa.gov/ics/advisories/icsa-20-170-02, https://us-cert.cisa.gov/ics/advisories/icsa-20-170-03	A-ICO-GENE-190820/293
Deserialization of Untrusted Data	16-Jul-20	5	A specially crafted communication packet sent to the affected systems could cause a denial-of-service condition due to improper deserialization. This issue affects: Mitsubishi Electric MC Works64 version 4.02C (10.95.208.31) and earlier, all versions; Mitsubishi Electric MC Works32 version 3.00A (9.50.255.02); ICONICS GenBroker64, Platform	https://www.us-cert.gov/ics/advisories/icsa-20-170-02, https://www.us-cert.gov/ics/advisories/icsa-20-170-03	A-ICO-GENE-190820/294

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Services, Workbench, FrameWorX Server version 10.96 and prior; ICONICS GenBroker32 version 9.5 and prior. **CVE ID : CVE-2020-12015**		
hyper_historian					
Deserialization of Untrusted Data	16-Jul-20	7.5	A specially crafted communication packet sent to the affected devices could allow remote code execution and a denial-of-service condition due to a deserialization vulnerability. This issue affects: Mitsubishi Electric MC Works64 version 4.02C (10.95.208.31) and earlier, all versions; Mitsubishi Electric MC Works32 version 3.00A (9.50.255.02); ICONICS GenBroker64, Platform Services, Workbench, FrameWorX Server version 10.96 and prior; ICONICS GenBroker32 version 9.5 and prior. **CVE ID : CVE-2020-12007**	https://us-cert.cisa.gov/ics/advisories/icsa-20-170-02,, https://us-cert.cisa.gov/ics/advisories/icsa-20-170-03	A-ICO-HYPE-190820/295
Deserialization of Untrusted Data	16-Jul-20	5	A specially crafted communication packet sent to the affected device could cause a denial-of-service condition due to a deserialization vulnerability. This affects: Mitsubishi Electric MC Works64 Version 4.02C (10.95.208.31) and earlier, all versions; Mitsubishi	https://us-cert.cisa.gov/ics/advisories/icsa-20-170-02, https://us-cert.cisa.gov/ics/advisories/icsa-20-170-03	A-ICO-HYPE-190820/296

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Electric MC Works32 Version 3.00A (9.50.255.02); ICONICS GenBroker64, Platform Services, Workbench, FrameWorX Server v10.96 and prior; ICONICS GenBroker32 v9.5 and prior. **CVE ID : CVE-2020-12009**		
Out-of-bounds Write	16-Jul-20	7.5	A specially crafted communication packet sent to the affected systems could cause a denial-of-service condition or allow remote code execution. This issue affects: Mitsubishi Electric MC Works64 version 4.02C (10.95.208.31) and earlier, all versions; MC Works32 version 3.00A (9.50.255.02); ICONICS GenBroker64, Platform Services, Workbench, FrameWorX Server version 10.96 and prior; GenBroker32 version 9.5 and prior. **CVE ID : CVE-2020-12011**	N/A	A-ICO-HYPE-190820/297
Improper Control of Generation of Code ('Code Injection')	16-Jul-20	6.4	A specially crafted WCF client that interfaces to the may allow the execution of certain arbitrary SQL commands remotely. This affects: Mitsubishi Electric MC Works64 Version 4.02C (10.95.208.31) and earlier, all versions; Mitsubishi Electric MC	https://us-cert.cisa.gov/ics/advisories/icsa-20-170-02, https://us-cert.cisa.gov/ics/advisories/icsa-20-170-03	A-ICO-HYPE-190820/298

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Works32 Version 3.00A (9.50.255.02); ICONICS GenBroker64, Platform Services, Workbench, FrameWorX Server v10.96 and prior; ICONICS GenBroker32 v9.5 and prior. **CVE ID : CVE-2020-12013**		
Deserialization of Untrusted Data	16-Jul-20	5	A specially crafted communication packet sent to the affected systems could cause a denial-of-service condition due to improper deserialization. This issue affects: Mitsubishi Electric MC Works64 version 4.02C (10.95.208.31) and earlier, all versions; Mitsubishi Electric MC Works32 version 3.00A (9.50.255.02); ICONICS GenBroker64, Platform Services, Workbench, FrameWorX Server version 10.96 and prior; ICONICS GenBroker32 version 9.5 and prior. **CVE ID : CVE-2020-12015**	https://www.us-cert.gov/ics/advisories/icsa-20-170-02, https://www.us-cert.gov/ics/advisories/icsa-20-170-03	A-ICO-HYPE-190820/299
mobilehmi					
Deserialization of Untrusted Data	16-Jul-20	7.5	A specially crafted communication packet sent to the affected devices could allow remote code execution and a denial-of-service condition due to a deserialization vulnerability. This issue affects: Mitsubishi Electric	https://us-cert.cisa.gov/ics/advisories/icsa-20-170-02,, https://us-cert.cisa.gov/ics/advisories/icsa-20-	A-ICO-MOBI-190820/300

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			MC Works64 version 4.02C (10.95.208.31) and earlier, all versions; Mitsubishi Electric MC Works32 version 3.00A (9.50.255.02); ICONICS GenBroker64, Platform Services, Workbench, FrameWorX Server version 10.96 and prior; ICONICS GenBroker32 version 9.5 and prior. **CVE ID : CVE-2020-12007**	170-03	
Deserialization of Untrusted Data	16-Jul-20	5	A specially crafted communication packet sent to the affected device could cause a denial-of-service condition due to a deserialization vulnerability. This affects: Mitsubishi Electric MC Works64 Version 4.02C (10.95.208.31) and earlier, all versions; Mitsubishi Electric MC Works32 Version 3.00A (9.50.255.02); ICONICS GenBroker64, Platform Services, Workbench, FrameWorX Server v10.96 and prior; ICONICS GenBroker32 v9.5 and prior. **CVE ID : CVE-2020-12009**	https://us-cert.cisa.gov/ics/advisories/icsa-20-170-02, https://us-cert.cisa.gov/ics/advisories/icsa-20-170-03	A-ICO-MOBI-190820/301
Out-of-bounds Write	16-Jul-20	7.5	A specially crafted communication packet sent to the affected systems could cause a denial-of-service condition or allow remote code	N/A	A-ICO-MOBI-190820/302

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			execution. This issue affects: Mitsubishi Electric MC Works64 version 4.02C (10.95.208.31) and earlier, all versions; MC Works32 version 3.00A (9.50.255.02); ICONICS GenBroker64, Platform Services, Workbench, FrameWorX Server version 10.96 and prior; GenBroker32 version 9.5 and prior. **CVE ID : CVE-2020-12011**		
Improper Control of Generation of Code ('Code Injection')	16-Jul-20	6.4	A specially crafted WCF client that interfaces to the may allow the execution of certain arbitrary SQL commands remotely. This affects: Mitsubishi Electric MC Works64 Version 4.02C (10.95.208.31) and earlier, all versions; Mitsubishi Electric MC Works32 Version 3.00A (9.50.255.02); ICONICS GenBroker64, Platform Services, Workbench, FrameWorX Server v10.96 and prior; ICONICS GenBroker32 v9.5 and prior. **CVE ID : CVE-2020-12013**	https://us-cert.cisa.gov/ics/advisories/icsa-20-170-02, https://us-cert.cisa.gov/ics/advisories/icsa-20-170-03	A-ICO-MOBI-190820/303
Deserialization of Untrusted Data	16-Jul-20	5	A specially crafted communication packet sent to the affected systems could cause a denial-of-service condition due to improper deserialization. This issue	https://www.us-cert.gov/ics/advisories/icsa-20-170-02, https://ww	A-ICO-MOBI-190820/304

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			affects: Mitsubishi Electric MC Works64 version 4.02C (10.95.208.31) and earlier, all versions; Mitsubishi Electric MC Works32 version 3.00A (9.50.255.02); ICONICS GenBroker64, Platform Services, Workbench, FrameWorX Server version 10.96 and prior; ICONICS GenBroker32 version 9.5 and prior. **CVE ID : CVE-2020-12015**	w.us-cert.gov/ics/advisories/icsa-20-170-03	
quality_analytix					
Deserialization of Untrusted Data	16-Jul-20	7.5	A specially crafted communication packet sent to the affected devices could allow remote code execution and a denial-of-service condition due to a deserialization vulnerability. This issue affects: Mitsubishi Electric MC Works64 version 4.02C (10.95.208.31) and earlier, all versions; Mitsubishi Electric MC Works32 version 3.00A (9.50.255.02); ICONICS GenBroker64, Platform Services, Workbench, FrameWorX Server version 10.96 and prior; ICONICS GenBroker32 version 9.5 and prior. **CVE ID : CVE-2020-12007**	https://us-cert.cisa.gov/ics/advisories/icsa-20-170-02,, https://us-cert.cisa.gov/ics/advisories/icsa-20-170-03	A-ICO-QUAL-190820/305
Deserialization of Untrusted	16-Jul-20	5	A specially crafted communication packet sent to the affected device	https://us-cert.cisa.gov/ics/advisorie	A-ICO-QUAL-190820/306

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Data			could cause a denial-of-service condition due to a deserialization vulnerability. This affects: Mitsubishi Electric MC Works64 Version 4.02C (10.95.208.31) and earlier, all versions; Mitsubishi Electric MC Works32 Version 3.00A (9.50.255.02); ICONICS GenBroker64, Platform Services, Workbench, FrameWorX Server v10.96 and prior; ICONICS GenBroker32 v9.5 and prior. **CVE ID : CVE-2020-12009**	s/icsa-20-170-02, https://us-cert.cisa.gov/ics/advisories/icsa-20-170-03	
Out-of-bounds Write	16-Jul-20	7.5	A specially crafted communication packet sent to the affected systems could cause a denial-of-service condition or allow remote code execution. This issue affects: Mitsubishi Electric MC Works64 version 4.02C (10.95.208.31) and earlier, all versions; MC Works32 version 3.00A (9.50.255.02); ICONICS GenBroker64, Platform Services, Workbench, FrameWorX Server version 10.96 and prior; GenBroker32 version 9.5 and prior. **CVE ID : CVE-2020-12011**	N/A	A-ICO-QUAL-190820/307
Improper Control of	16-Jul-20	6.4	A specially crafted WCF client that interfaces to the	https://us-cert.cisa.gov/	A-ICO-QUAL-190820/308

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Generation of Code ('Code Injection')			may allow the execution of certain arbitrary SQL commands remotely. This affects: Mitsubishi Electric MC Works64 Version 4.02C (10.95.208.31) and earlier, all versions; Mitsubishi Electric MC Works32 Version 3.00A (9.50.255.02); ICONICS GenBroker64, Platform Services, Workbench, FrameWorX Server v10.96 and prior; ICONICS GenBroker32 v9.5 and prior. **CVE ID : CVE-2020-12013**	ics/advisories/icsa-20-170-02, https://us-cert.cisa.gov/ics/advisories/icsa-20-170-03	
Deserialization of Untrusted Data	16-Jul-20	5	A specially crafted communication packet sent to the affected systems could cause a denial-of-service condition due to improper deserialization. This issue affects: Mitsubishi Electric MC Works64 version 4.02C (10.95.208.31) and earlier, all versions; Mitsubishi Electric MC Works32 version 3.00A (9.50.255.02); ICONICS GenBroker64, Platform Services, Workbench, FrameWorX Server version 10.96 and prior; ICONICS GenBroker32 version 9.5 and prior. **CVE ID : CVE-2020-12015**	https://www.us-cert.gov/ics/advisories/icsa-20-170-02, https://www.us-cert.gov/ics/advisories/icsa-20-170-03	A-ICO-QUAL-190820/309
smart_energy_analytix					

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Deserialization of Untrusted Data	16-Jul-20	7.5	A specially crafted communication packet sent to the affected devices could allow remote code execution and a denial-of-service condition due to a deserialization vulnerability. This issue affects: Mitsubishi Electric MC Works64 version 4.02C (10.95.208.31) and earlier, all versions; Mitsubishi Electric MC Works32 version 3.00A (9.50.255.02); ICONICS GenBroker64, Platform Services, Workbench, FrameWorX Server version 10.96 and prior; ICONICS GenBroker32 version 9.5 and prior. **CVE ID : CVE-2020-12007**	https://us-cert.cisa.gov/ics/advisories/icsa-20-170-02,, https://us-cert.cisa.gov/ics/advisories/icsa-20-170-03	A-ICO-SMAR-190820/310
Deserialization of Untrusted Data	16-Jul-20	5	A specially crafted communication packet sent to the affected device could cause a denial-of-service condition due to a deserialization vulnerability. This affects: Mitsubishi Electric MC Works64 Version 4.02C (10.95.208.31) and earlier, all versions; Mitsubishi Electric MC Works32 Version 3.00A (9.50.255.02); ICONICS GenBroker64, Platform Services, Workbench, FrameWorX Server v10.96 and prior; ICONICS GenBroker32 v9.5 and	https://us-cert.cisa.gov/ics/advisories/icsa-20-170-02, https://us-cert.cisa.gov/ics/advisories/icsa-20-170-03	A-ICO-SMAR-190820/311

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			prior. **CVE ID : CVE-2020-12009**		
Out-of-bounds Write	16-Jul-20	7.5	A specially crafted communication packet sent to the affected systems could cause a denial-of-service condition or allow remote code execution. This issue affects: Mitsubishi Electric MC Works64 version 4.02C (10.95.208.31) and earlier, all versions; MC Works32 version 3.00A (9.50.255.02); ICONICS GenBroker64, Platform Services, Workbench, FrameWorX Server version 10.96 and prior; GenBroker32 version 9.5 and prior. **CVE ID : CVE-2020-12011**	N/A	A-ICO-SMAR-190820/312
Improper Control of Generation of Code ('Code Injection')	16-Jul-20	6.4	A specially crafted WCF client that interfaces to the may allow the execution of certain arbitrary SQL commands remotely. This affects: Mitsubishi Electric MC Works64 Version 4.02C (10.95.208.31) and earlier, all versions; Mitsubishi Electric MC Works32 Version 3.00A (9.50.255.02); ICONICS GenBroker64, Platform Services, Workbench, FrameWorX Server v10.96 and prior; ICONICS GenBroker32 v9.5 and prior.	https://us-cert.cisa.gov/ics/advisories/icsa-20-170-02, https://us-cert.cisa.gov/ics/advisories/icsa-20-170-03	A-ICO-SMAR-190820/313

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2020-12013		
Deserialization of Untrusted Data	16-Jul-20	5	A specially crafted communication packet sent to the affected systems could cause a denial-of-service condition due to improper deserialization. This issue affects: Mitsubishi Electric MC Works64 version 4.02C (10.95.208.31) and earlier, all versions; Mitsubishi Electric MC Works32 version 3.00A (9.50.255.02); ICONICS GenBroker64, Platform Services, Workbench, FrameWorX Server version 10.96 and prior; ICONICS GenBroker32 version 9.5 and prior. **CVE ID : CVE-2020-12015**	https://www.us-cert.gov/ics/advisories/icsa-20-170-02, https://www.us-cert.gov/ics/advisories/icsa-20-170-03	A-ICO-SMAR-190820/314
bizviz					
Deserialization of Untrusted Data	16-Jul-20	7.5	A specially crafted communication packet sent to the affected devices could allow remote code execution and a denial-of-service condition due to a deserialization vulnerability. This issue affects: Mitsubishi Electric MC Works64 version 4.02C (10.95.208.31) and earlier, all versions; Mitsubishi Electric MC Works32 version 3.00A (9.50.255.02); ICONICS GenBroker64, Platform Services, Workbench,	https://us-cert.cisa.gov/ics/advisories/icsa-20-170-02,, https://us-cert.cisa.gov/ics/advisories/icsa-20-170-03	A-ICO-BIZV-190820/315

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			FrameWorX Server version 10.96 and prior; ICONICS GenBroker32 version 9.5 and prior. **CVE ID : CVE-2020-12007**		
Deserialization of Untrusted Data	16-Jul-20	5	A specially crafted communication packet sent to the affected device could cause a denial-of-service condition due to a deserialization vulnerability. This affects: Mitsubishi Electric MC Works64 Version 4.02C (10.95.208.31) and earlier, all versions; Mitsubishi Electric MC Works32 Version 3.00A (9.50.255.02); ICONICS GenBroker64, Platform Services, Workbench, FrameWorX Server v10.96 and prior; ICONICS GenBroker32 v9.5 and prior. **CVE ID : CVE-2020-12009**	https://us-cert.cisa.gov/ics/advisories/icsa-20-170-02, https://us-cert.cisa.gov/ics/advisories/icsa-20-170-03	A-ICO-BIZV-190820/316
Out-of-bounds Write	16-Jul-20	7.5	A specially crafted communication packet sent to the affected systems could cause a denial-of-service condition or allow remote code execution. This issue affects: Mitsubishi Electric MC Works64 version 4.02C (10.95.208.31) and earlier, all versions; MC Works32 version 3.00A (9.50.255.02); ICONICS GenBroker64, Platform	N/A	A-ICO-BIZV-190820/317

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Services, Workbench, FrameWorX Server version 10.96 and prior; GenBroker32 version 9.5 and prior. **CVE ID : CVE-2020-12011**		
Improper Control of Generation of Code ('Code Injection')	16-Jul-20	6.4	A specially crafted WCF client that interfaces to the may allow the execution of certain arbitrary SQL commands remotely. This affects: Mitsubishi Electric MC Works64 Version 4.02C (10.95.208.31) and earlier, all versions; Mitsubishi Electric MC Works32 Version 3.00A (9.50.255.02); ICONICS GenBroker64, Platform Services, Workbench, FrameWorX Server v10.96 and prior; ICONICS GenBroker32 v9.5 and prior. **CVE ID : CVE-2020-12013**	https://us-cert.cisa.gov/ics/advisories/icsa-20-170-02, https://us-cert.cisa.gov/ics/advisories/icsa-20-170-03	A-ICO-BIZV-190820/318
Deserialization of Untrusted Data	16-Jul-20	5	A specially crafted communication packet sent to the affected systems could cause a denial-of-service condition due to improper deserialization. This issue affects: Mitsubishi Electric MC Works64 version 4.02C (10.95.208.31) and earlier, all versions; Mitsubishi Electric MC Works32 version 3.00A (9.50.255.02); ICONICS GenBroker64, Platform	https://www.us-cert.gov/ics/advisories/icsa-20-170-02, https://www.us-cert.gov/ics/advisories/icsa-20-170-03	A-ICO-BIZV-190820/319

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Services, Workbench, FrameWorX Server version 10.96 and prior; ICONICS GenBroker32 version 9.5 and prior. **CVE ID : CVE-2020-12015**		
genesis32					
Deserialization of Untrusted Data	16-Jul-20	7.5	A specially crafted communication packet sent to the affected devices could allow remote code execution and a denial-of-service condition due to a deserialization vulnerability. This issue affects: Mitsubishi Electric MC Works64 version 4.02C (10.95.208.31) and earlier, all versions; Mitsubishi Electric MC Works32 version 3.00A (9.50.255.02); ICONICS GenBroker64, Platform Services, Workbench, FrameWorX Server version 10.96 and prior; ICONICS GenBroker32 version 9.5 and prior. **CVE ID : CVE-2020-12007**	https://us-cert.cisa.gov/ics/advisories/icsa-20-170-02,, https://us-cert.cisa.gov/ics/advisories/icsa-20-170-03	A-ICO-GENE-190820/320
Deserialization of Untrusted Data	16-Jul-20	5	A specially crafted communication packet sent to the affected device could cause a denial-of-service condition due to a deserialization vulnerability. This affects: Mitsubishi Electric MC Works64 Version 4.02C (10.95.208.31) and earlier, all versions; Mitsubishi	https://us-cert.cisa.gov/ics/advisories/icsa-20-170-02, https://us-cert.cisa.gov/ics/advisories/icsa-20-170-03	A-ICO-GENE-190820/321

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Electric MC Works32 Version 3.00A (9.50.255.02); ICONICS GenBroker64, Platform Services, Workbench, FrameWorX Server v10.96 and prior; ICONICS GenBroker32 v9.5 and prior. **CVE ID : CVE-2020-12009**		
Out-of-bounds Write	16-Jul-20	7.5	A specially crafted communication packet sent to the affected systems could cause a denial-of-service condition or allow remote code execution. This issue affects: Mitsubishi Electric MC Works64 version 4.02C (10.95.208.31) and earlier, all versions; MC Works32 version 3.00A (9.50.255.02); ICONICS GenBroker64, Platform Services, Workbench, FrameWorX Server version 10.96 and prior; GenBroker32 version 9.5 and prior. **CVE ID : CVE-2020-12011**	N/A	A-ICO-GENE-190820/322
Improper Control of Generation of Code ('Code Injection')	16-Jul-20	6.4	A specially crafted WCF client that interfaces to the may allow the execution of certain arbitrary SQL commands remotely. This affects: Mitsubishi Electric MC Works64 Version 4.02C (10.95.208.31) and earlier, all versions; Mitsubishi Electric MC	https://us-cert.cisa.gov/ics/advisories/icsa-20-170-02, https://us-cert.cisa.gov/ics/advisories/icsa-20-170-03	A-ICO-GENE-190820/323

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Works32 Version 3.00A (9.50.255.02); ICONICS GenBroker64, Platform Services, Workbench, FrameWorX Server v10.96 and prior; ICONICS GenBroker32 v9.5 and prior. **CVE ID : CVE-2020-12013**		
Deserialization of Untrusted Data	16-Jul-20	5	A specially crafted communication packet sent to the affected systems could cause a denial-of-service condition due to improper deserialization. This issue affects: Mitsubishi Electric MC Works64 version 4.02C (10.95.208.31) and earlier, all versions; Mitsubishi Electric MC Works32 version 3.00A (9.50.255.02); ICONICS GenBroker64, Platform Services, Workbench, FrameWorX Server version 10.96 and prior; ICONICS GenBroker32 version 9.5 and prior. **CVE ID : CVE-2020-12015**	https://www.us-cert.gov/ics/advisories/icsa-20-170-02, https://www.us-cert.gov/ics/advisories/icsa-20-170-03	A-ICO-GENE-190820/324
ihatemoney					
i_hate_money					
Incorrect Authorization	27-Jul-20	4	In "I hate money" before version 4.1.5, an authenticated member of one project can modify and delete members of another project, without knowledge of this other	https://github.com/spiral-project/ihatemoney/security/advisories/GHSA-	A-IHA-I_HA-190820/325

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			project's private code. This can be further exploited to access all bills of another project without knowledge of this other project's private code. With the default configuration, anybody is allowed to create a new project. An attacker can create a new project and then use it to become authenticated and exploit this flaw. As such, the exposure is similar to an unauthenticated attack, because it is trivial to become authenticated. This is fixed in version 4.1.5. **CVE ID : CVE-2020-15120**	67j9-c52g-w2q9	
indo-mars					
marscode					
Improper Limitation of a Pathname to a Restricted Directory ('Path Traversal')	25-Jul-20	5	This affects all versions of package marscode. There is no path sanitization in the path provided at fs.readFile in index.js. **CVE ID : CVE-2020-7681**	N/A	A-IND-MARS-190820/326
Inductiveautomation					
ignition_gateway					
Missing Authorizatio n	31-Jul-20	5	The affected product is vulnerable to an information leak, which may allow an attacker to obtain sensitive information on the Ignition 8 (all versions prior to	N/A	A-IND-IGNI-190820/327

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			8.0.13). **CVE ID : CVE-2020-14520**		
inneo					
startup_tools					
Improper Limitation of a Pathname to a Restricted Directory ('Path Traversal')	23-Jul-20	7.5	An issue was discovered in INNEO Startup TOOLS 2017 M021 12.0.66.3784 through 2018 M040 13.0.70.3804. The sut_srv.exe web application (served on TCP port 85) includes user input into a filesystem access without any further validation. This might allow an unauthenticated attacker to read files on the server via Directory Traversal, or possibly have unspecified other impact. **CVE ID : CVE-2020-15492**	https://www.inneo.de/files/content/Produktentwicklung/Tools-und-Erweiterungen/Startup-TOOLS/INNEO-SA-SUT-2020-01.pdf	A-INN-STAR-190820/328
intranda					
goobi_viewer_core					
Improper Limitation of a Pathname to a Restricted Directory ('Path Traversal')	22-Jul-20	4	In Goobi Viewer Core before version 4.8.3, a path traversal vulnerability allows for remote attackers to access files on the server via the application. This is limited to files accessible to the application server user, eg. tomcat, but can potentially lead to the disclosure of sensitive information. The vulnerability has been fixed in version 4.8.3 **CVE ID : CVE-2020-15124**	https://github.com/intranda/goobi-viewer-core/security/advisories/GHSA-7gwq-xqw3-cr63	A-INT-GOOB-190820/329

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
jalios					
jcms					
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	17-Jul-20	4.3	** DISPUTED ** jcore/portal/ajaxPortal.jsp in Jalios JCMS 10.0.2 build-20200224104759 allows XSS via the types parameter. Note: It is asserted that this vulnerability is not present in the standard installation of Jalios JCMS. **CVE ID : CVE-2020-15497**	N/A	A-JAL-JCMS-190820/330
jpeg-js_project					
jpeg-js					
Uncontrolled Resource Consumption	24-Jul-20	4.3	Uncontrolled resource consumption in `jpeg-js` before 0.4.0 may allow attacker to launch denial of service attacks using specially a crafted JPEG image. **CVE ID : CVE-2020-8175**	N/A	A-JPE-JPEG-190820/331
Juniper					
junos					
Improper Restriction of Operations within the Bounds of a Memory Buffer	17-Jul-20	5	On Juniper Networks Junos OS devices, a stream of TCP packets sent to the Routing Engine (RE) may cause mbuf leak which can lead to Flexible PIC Concentrator (FPC) crash or the system to crash and restart (vmcore). This issue can be trigged by IPv4 or IPv6 and it is caused only by TCP packets. This issue is not	https://kb.juniper.net/JSA11040	A-JUN-JUNO-190820/332

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			related to any specific configuration and it affects Junos OS releases starting from 17.4R1. However, this issue does not affect Junos OS releases prior to 18.2R1 when Nonstop active routing (NSR) is configured [edit routing-options nonstop-routing]. The number of mbufs is platform dependent. The following command provides the number of mbufs counter that are currently in use and maximum number of mbufs that can be allocated on a platform: user@host> show system buffers 2437/3143/5580 mbufs in use (current/cache/total) Once the device runs out of mbufs, the FPC crashes or the vmcore occurs and the device might become inaccessible requiring a manual restart. This issue affects Juniper Networks Junos OS 17.4 versions prior to 17.4R2-S11, 17.4R3-S2; 18.1 versions prior to 18.1R3-S10; 18.2 versions prior to 18.2R2-S7, 18.2R3-S5; 18.2X75 versions prior to 18.2X75-D41, 18.2X75-D420.12, 18.2X75-D51, 18.2X75-D60, 18.2X75-D34; 18.3 versions prior to 18.3R2-		

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			S4, 18.3R3-S2; 18.4 versions prior to 18.4R1-S7, 18.4R2-S4, 18.4R3-S1; 19.1 versions prior to 19.1R1-S5, 19.1R2-S1, 19.1R3; 19.2 versions prior to 19.2R1-S5, 19.2R2; 19.3 versions prior to 19.3R2-S3, 19.3R3; 19.4 versions prior to 19.4R1-S2, 19.4R2. Versions of Junos OS prior to 17.4R1 are unaffected by this vulnerability. **CVE ID : CVE-2020-1653**		
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	17-Jul-20	7.5	On Juniper Networks SRX Series with ICAP (Internet Content Adaptation Protocol) redirect service enabled, processing a malformed HTTP message can lead to a Denial of Service (DoS) or Remote Code Execution (RCE) Continued processing of this malformed HTTP message may result in an extended Denial of Service (DoS) condition. The offending HTTP message that causes this issue may originate both from the HTTP server or the HTTP client. This issue affects Juniper Networks Junos OS on SRX Series: 18.1 versions prior to 18.1R3-S9 ; 18.2 versions prior to 18.2R2-S7, 18.2R3-S3; 18.3 versions prior to 18.3R1-S7, 18.3R2-S4,	https://kb.juniper.net/JSA11031	A-JUN-JUNO-190820/333

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			18.3R3-S1; 18.4 versions prior to 18.4R1-S7, 18.4R2-S4, 18.4R3; 19.1 versions prior to 19.1R1-S5, 19.1R2; 19.2 versions prior to 19.2R1-S2, 19.2R2; 19.3 versions prior to 19.3R2. This issue does not affect Juniper Networks Junos OS prior to 18.1R1. **CVE ID : CVE-2020-1654**		
jupyterhub					
kubespawner					
Incorrect Authorization	17-Jul-20	5.5	In jupyterhub-kubespawner before 0.12, certain usernames will be able to craft particular server names which will grant them access to the default server of other users who have matching usernames. This has been fixed in 0.12. **CVE ID : CVE-2020-15110**	https://github.com/jupyterhub/kubespawner/commit/3dfe870a7f5e98e2e398b01996ca6b8eff4bb1d0, https://github.com/jupyterhub/kubespawner/security/advisories/GHSA-v7m9-9497-p9gr	A-JUP-KUBE-190820/334
KDE					
kmail					
Cleartext Transmission of Sensitive Information	27-Jul-20	4.3	KDE KMail 19.12.3 (aka 5.13.3) engages in unencrypted POP3 communication during times when the UI indicates that encryption	N/A	A-KDE-KMAI-190820/335

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			is in use. **CVE ID : CVE-2020-15954**		
kitodo					
kitodo.presentation					
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	29-Jul-20	4.3	The dlf (aka Kitodo.Presentation) extension before 3.1.2 for TYPO3 allows XSS. **CVE ID : CVE-2020-16095**	https://typo3.org/security/advisory/typo3-ext-sa-2020-015	A-KIT-KITO-190820/336
kramdown_project					
kramdown					
Improper Neutralization of Special Elements in Output Used by a Downstream Component ('Injection')	17-Jul-20	7.5	The kramdown gem before 2.3.0 for Ruby processes the template option inside Kramdown documents by default, which allows unintended read access (such as template="/etc/passwd") or unintended embedded Ruby code execution (such as a string that begins with template="string://<%= `). NOTE: kramdown is used in Jekyll, GitLab Pages, GitHub Pages, and Thredded Forum. **CVE ID : CVE-2020-14001**	https://github.com/gettalong/kramdown/commit/1b8fd33c3120bfc6e5164b449e2c2fc9c9306fde, https://github.com/gettalong/kramdown/compare/REL_2_2_1...REL_2_3_0, https://kramdown.gettalong.org/news.html, https://security.netapp.com/advisory/ntap-20200731-0004/	A-KRA-KRAM-190820/337

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Kubernetes					
kubernetes					
Uncontrolled Resource Consumption	23-Jul-20	2.1	The Kubernetes kubelet component in versions 1.1-1.16.12, 1.17.0-1.17.8 and 1.18.0-1.18.5 do not account for disk usage by a pod which writes to its own /etc/hosts file. The /etc/hosts file mounted in a pod by kubelet is not included by the kubelet eviction manager when calculating ephemeral storage usage by a pod. If a pod writes a large amount of data to the /etc/hosts file, it could fill the storage space of the node and cause the node to fail. **CVE ID : CVE-2020-8557**	https://github.com/kubernetes/kubernetes/issues/93032	A-KUB-KUBE-190820/338
Improper Authentication	27-Jul-20	5.8	The Kubelet and kube-proxy components in versions 1.1.0-1.16.10, 1.17.0-1.17.6, and 1.18.0-1.18.3 were found to contain a security issue which allows adjacent hosts to reach TCP and UDP services bound to 127.0.0.1 running on the node or in the node's network namespace. Such a service is generally thought to be reachable only by other processes on the same host, but due to this defeect, could be reachable by other hosts on the same LAN as the	https://github.com/kubernetes/kubernetes/issues/92315	A-KUB-KUBE-190820/339

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			node, or by containers running on the same node as the service. **CVE ID : CVE-2020-8558**		
URL Redirection to Untrusted Site ('Open Redirect')	22-Jul-20	6	The Kubernetes kube-apiserver in versions v1.6-v1.15, and versions prior to v1.16.13, v1.17.9 and v1.18.6 are vulnerable to an unvalidated redirect on proxied upgrade requests that could allow an attacker to escalate privileges from a node compromise to a full cluster compromise. **CVE ID : CVE-2020-8559**	https://security.netapp.com/advisory/ntap-20200810-0004/	A-KUB-KUBE-190820/340
ingress-nginx					
Externally Controlled Reference to a Resource in Another Sphere	29-Jul-20	4.9	The Kubernetes ingress-nginx component prior to version 0.28.0 allows a user with the ability to create namespaces and to read and create ingress objects to overwrite the password file of another ingress which uses nginx.ingress.kubernetes.io/auth-type: basic and which has a hyphenated namespace or secret name. **CVE ID : CVE-2020-8553**	https://github.com/kubernetes/ingress-nginx/issues/5126	A-KUB-INGR-190820/341
kubevirt					
kubevirt					
Improper Privilege Management	29-Jul-20	6.5	A flaw was found in kubevirt 0.29 and earlier. Virtual Machine Instances (VMIs) can be used to gain	N/A	A-KUB-KUBE-190820/342

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			access to the host's filesystem. Successful exploitation allows an attacker to assume the privileges of the VM process on the host system. In worst-case scenarios an attacker can read and modify any file on the system where the VMI is running. The highest threat from this vulnerability is to data confidentiality and integrity as well as system availability. **CVE ID : CVE-2020-14316**		
kujirahand					
konawiki					
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	29-Jul-20	4.3	Cross-site scripting vulnerability in KonaWiki 2.2.0 and earlier allows remote attackers to execute an arbitrary script via a specially crafted URL. **CVE ID : CVE-2020-5612**	N/A	A-KUJ-KONA-190820/343
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	29-Jul-20	4.3	Cross-site scripting vulnerability in KonaWiki 3.1.0 and earlier allows remote attackers to execute an arbitrary script via a specially crafted URL. **CVE ID : CVE-2020-5613**	N/A	A-KUJ-KONA-190820/344
Improper Limitation of a Pathname to a	29-Jul-20	5	Directory traversal vulnerability in KonaWiki 3.1.0 and earlier allows remote attackers to read	N/A	A-KUJ-KONA-190820/345

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Restricted Directory ('Path Traversal')			arbitrary files via unspecified vectors. **CVE ID : CVE-2020-5614**		
Lenovo					
drivers_management					
Untrusted Search Path	24-Jul-20	6.9	A DLL search path vulnerability was reported in Lenovo Drivers Management prior to version 2.7.1128.1046 that could allow an authenticated user to execute code with elevated privileges. **CVE ID : CVE-2020-8317**	https://iknow.lenovo.com.cn/detail/dc_190088.html	A-LEN-DRIV-190820/346
Unquoted Search Path or Element	24-Jul-20	6.9	An unquoted service path vulnerability was reported in Lenovo Drivers Management prior to version 2.7.1128.1046 that could allow an authenticated user to execute code with elevated privileges. **CVE ID : CVE-2020-8326**	https://iknow.lenovo.com.cn/detail/dc_190088.html	A-LEN-DRIV-190820/347
libetpan_project					
libetpan					
Improper Neutralization of Special Elements in Output Used by a Downstream Component ('Injection')	27-Jul-20	5.8	LibEtPan through 1.9.4, as used in MailCore 2 through 0.6.3 and other products, has a STARTTLS buffering issue that affects IMAP, SMTP, and POP3. When a server sends a "begin TLS" response, the client reads additional data (e.g., from a meddler-in-the-middle	N/A	A-LIB-LIBE-190820/348

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			attacker) and evaluates it in a TLS context, aka "response injection." **CVE ID : CVE-2020-15953**		
libmailcore					
mailcore2					
Improper Neutralization of Special Elements in Output Used by a Downstream Component ('Injection')	27-Jul-20	5.8	LibEtPan through 1.9.4, as used in MailCore 2 through 0.6.3 and other products, has a STARTTLS buffering issue that affects IMAP, SMTP, and POP3. When a server sends a "begin TLS" response, the client reads additional data (e.g., from a meddler-in-the-middle attacker) and evaluates it in a TLS context, aka "response injection." **CVE ID : CVE-2020-15953**	N/A	A-LIB-MAIL-190820/349
librenms					
librenms					
Improper Neutralization of Special Elements used in an SQL Command ('SQL Injection')	21-Jul-20	4	In LibreNMS before 1.65.1, an authenticated attacker can achieve SQL Injection via the customoid.inc.php device_id POST parameter to ajax_form.php. **CVE ID : CVE-2020-15873**	N/A	A-LIB-LIBR-190820/350
Exposure of Resource to Wrong Sphere	21-Jul-20	6.5	An issue was discovered in LibreNMS before 1.65.1. It has insufficient access control for normal users because of "'guard' => 'admin'" instead of "'middleware' =>	N/A	A-LIB-LIBR-190820/351

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			['can:admin']" in routes/web.php. **CVE ID : CVE-2020-15877**		
Libssh					
libssh					
NULL Pointer Dereference	29-Jul-20	4.3	libssh 0.9.4 has a NULL pointer dereference in tftpserver.c if ssh_buffer_new returns NULL. **CVE ID : CVE-2020-16135**	N/A	A-LIB-LIBS-190820/352
Liferay					
liferay_portal					
Insufficiently Protected Credentials	20-Jul-20	4.3	Liferay Portal before 7.3.0, and Liferay DXP 7.0 before fix pack 89, 7.1 before fix pack 17, and 7.2 before fix pack 4, does not safely test a connection to a LDAP server, which allows remote attackers to obtain the LDAP server's password via the Test LDAP Connection feature. **CVE ID : CVE-2020-15841**	N/A	A-LIF-LIFE-190820/353
Deserialization of Untrusted Data	20-Jul-20	6.8	Liferay Portal before 7.3.0, and Liferay DXP 7.0 before fix pack 90, 7.1 before fix pack 17, and 7.2 before fix pack 5, allows man-in-the-middle attackers to execute arbitrary code via crafted serialized payloads, because of insecure deserialization. **CVE ID : CVE-2020-15842**	N/A	A-LIF-LIFE-190820/354
dxp					

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Insufficiently Protected Credentials	20-Jul-20	4.3	Liferay Portal before 7.3.0, and Liferay DXP 7.0 before fix pack 89, 7.1 before fix pack 17, and 7.2 before fix pack 4, does not safely test a connection to a LDAP server, which allows remote attackers to obtain the LDAP server's password via the Test LDAP Connection feature. **CVE ID : CVE-2020-15841**	N/A	A-LIF-DXP-190820/355
Deserialization of Untrusted Data	20-Jul-20	6.8	Liferay Portal before 7.3.0, and Liferay DXP 7.0 before fix pack 90, 7.1 before fix pack 17, and 7.2 before fix pack 5, allows man-in-the-middle attackers to execute arbitrary code via crafted serialized payloads, because of insecure deserialization. **CVE ID : CVE-2020-15842**	N/A	A-LIF-DXP-190820/356
LUA					
lua					
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	21-Jul-20	6.8	Lua through 5.4.0 mishandles the interaction between stack resizes and garbage collection, leading to a heap-based buffer overflow, heap-based buffer over-read, or use-after-free. **CVE ID : CVE-2020-15888**	N/A	A-LUA-LUA-190820/357
Out-of-bounds Read	21-Jul-20	7.5	Lua through 5.4.0 has a getobjname heap-based buffer over-read because youngcollection in lgc.c uses markold for an	N/A	A-LUA-LUA-190820/358

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			insufficient number of list members. **CVE ID : CVE-2020-15889**		
N/A	24-Jul-20	2.1	Lua through 5.4.0 has a segmentation fault in changedline in ldebug.c (e.g., when called by luaG_traceexec) because it incorrectly expects that an oldpc value is always updated upon a return of the flow of control to a function. **CVE ID : CVE-2020-15945**	N/A	A-LUA-LUA-190820/359
luajit					
luajit					
Out-of-bounds Read	21-Jul-20	5	LuaJit through 2.1.0-beta3 has an out-of-bounds read because __gc handler frame traversal is mishandled. **CVE ID : CVE-2020-15890**	N/A	A-LUA-LUAJ-190820/360
Magento					
magento					
Improper Control of Generation of Code ('Code Injection')	22-Jul-20	7.5	Magento versions 1.14.4.5 and earlier, and 1.9.4.5 and earlier have a php object injection vulnerability. Successful exploitation could lead to arbitrary code execution. **CVE ID : CVE-2020-9664**	https://helpx.adobe.com/security/products/magento/apsb20-41.html	A-MAG-MAGE-190820/361
Improper Neutralization of Input During Web Page	22-Jul-20	4.3	Magento versions 1.14.4.5 and earlier, and 1.9.4.5 and earlier have a stored cross-site scripting vulnerability. Successful exploitation	https://helpx.adobe.com/security/products/magento/apsb20-	A-MAG-MAGE-190820/362

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Generation ('Cross-site Scripting')			could lead to sensitive information disclosure. **CVE ID : CVE-2020-9665**	41.html	
Improper Limitation of a Pathname to a Restricted Directory ('Path Traversal')	29-Jul-20	8.5	Magento versions 2.3.5-p1 and earlier, and 2.3.5-p1 and earlier have a path traversal vulnerability. Successful exploitation could lead to arbitrary code execution. **CVE ID : CVE-2020-9689**	https://helpx.adobe.com/security/products/magento/apsb20-47.html	A-MAG-MAGE-190820/363
Information Exposure Through Discrepancy	29-Jul-20	3.5	Magento versions 2.3.5-p1 and earlier, and 2.3.5-p1 and earlier have an observable timing discrepancy vulnerability. Successful exploitation could lead to signature verification bypass. **CVE ID : CVE-2020-9690**	https://helpx.adobe.com/security/products/magento/apsb20-47.html	A-MAG-MAGE-190820/364
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	29-Jul-20	9.3	Magento versions 2.3.5-p1 and earlier, and 2.3.5-p1 and earlier have a dom-based cross-site scripting vulnerability. Successful exploitation could lead to arbitrary code execution. **CVE ID : CVE-2020-9691**	https://helpx.adobe.com/security/products/magento/apsb20-47.html	A-MAG-MAGE-190820/365
Incorrect Authorization	29-Jul-20	8.5	Magento versions 2.3.5-p1 and earlier, and 2.3.5-p1 and earlier have a security mitigation bypass vulnerability. Successful exploitation could lead to arbitrary code execution. **CVE ID : CVE-2020-9692**	https://helpx.adobe.com/security/products/magento/apsb20-47.html	A-MAG-MAGE-190820/366
marked-tree_project					

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
marked-tree					
Improper Limitation of a Pathname to a Restricted Directory ('Path Traversal')	25-Jul-20	5	This affects all versions of package marked-tree. There is no path sanitization in the path provided at fs.readFile in index.js. **CVE ID : CVE-2020-7682**	N/A	A-MAR-MARK-190820/367
Microweber					
microweber					
Information Exposure	16-Jul-20	5	userfiles/modules/users/controller/controller.php in Microweber before 1.1.20 allows an unauthenticated user to disclose the users database via a /modules/ POST request. **CVE ID : CVE-2020-13405**	N/A	A-MIC-MICR-190820/368
midasolutions					
eframework					
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	24-Jul-20	3.5	Multiple Stored Cross Site Scripting (XSS) vulnerabilities were discovered in Mida eFramework through 2.9.0. **CVE ID : CVE-2020-15918**	N/A	A-MID-EFRA-190820/369
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	24-Jul-20	4.3	A Reflected Cross Site Scripting (XSS) vulnerability was discovered in Mida eFramework through 2.9.0. **CVE ID : CVE-2020-15919**	N/A	A-MID-EFRA-190820/370
Improper	24-Jul-20	10	There is an OS Command	N/A	A-MID-EFRA-

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Neutralization of Special Elements used in an OS Command ('OS Command Injection')			Injection in Mida eFramework through 2.9.0 that allows an attacker to achieve Remote Code Execution (RCE) with administrative (root) privileges. No authentication is required. **CVE ID : CVE-2020-15920**		190820/371
Insufficiently Protected Credentials	24-Jul-20	7.5	Mida eFramework through 2.9.0 has a back door that permits a change of the administrative password and access to restricted functionalities, such as Code Execution. **CVE ID : CVE-2020-15921**	N/A	A-MID-EFRA-190820/372
Improper Neutralization of Special Elements used in an OS Command ('OS Command Injection')	24-Jul-20	10	There is an OS Command Injection in Mida eFramework 2.9.0 that allows an attacker to achieve Remote Code Execution (RCE) with administrative (root) privileges. Authentication is required. **CVE ID : CVE-2020-15922**	N/A	A-MID-EFRA-190820/373
Improper Limitation of a Pathname to a Restricted Directory ('Path Traversal')	24-Jul-20	7.8	Mida eFramework through 2.9.0 allows unauthenticated ../ directory traversal. **CVE ID : CVE-2020-15923**	N/A	A-MID-EFRA-190820/374
Improper Neutralization of Special Elements	24-Jul-20	5	There is a SQL Injection in Mida eFramework through 2.9.0 that leads to Information Disclosure. No	N/A	A-MID-EFRA-190820/375

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
used in an SQL Command ('SQL Injection')			authentication is required. The injection point resides in one of the authentication parameters. **CVE ID : CVE-2020-15924**		
MIT					
scratch-vm					
Deserialization of Untrusted Data	16-Jul-20	7.5	MIT Lifelong Kindergarten Scratch scratch-vm before 0.2.0-prerelease.20200714185213 loads extension URLs from untrusted project.json files with certain _ characters, resulting in remote code execution because the URL's content is treated as a script and is executed as a worker. The responsible code is getExtensionIdForOpcode in serialization/sb3.js. The use of _ is incompatible with a protection mechanism in older versions, in which URLs were split and consequently deserialization attacks were prevented. NOTE: the scratch.mit.edu hosted service is not affected because of the lack of worker scripts. **CVE ID : CVE-2020-14000**	https://github.com/LLK/scratch-vm/pull/2476, https://scratch.mit.edu/discuss/topic/422904/?page=1#post-4223443	A-MIT-SCRA-190820/376
Mitsubishielectric					
mc_works					

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Deserialization of Untrusted Data	16-Jul-20	7.5	A specially crafted communication packet sent to the affected devices could allow remote code execution and a denial-of-service condition due to a deserialization vulnerability. This issue affects: Mitsubishi Electric MC Works64 version 4.02C (10.95.208.31) and earlier, all versions; Mitsubishi Electric MC Works32 version 3.00A (9.50.255.02); ICONICS GenBroker64, Platform Services, Workbench, FrameWorX Server version 10.96 and prior; ICONICS GenBroker32 version 9.5 and prior. **CVE ID : CVE-2020-12007**	https://us-cert.cisa.gov/ics/advisories/icsa-20-170-02,, https://us-cert.cisa.gov/ics/advisories/icsa-20-170-03	A-MIT-MC_W-190820/377
Deserialization of Untrusted Data	16-Jul-20	5	A specially crafted communication packet sent to the affected device could cause a denial-of-service condition due to a deserialization vulnerability. This affects: Mitsubishi Electric MC Works64 Version 4.02C (10.95.208.31) and earlier, all versions; Mitsubishi Electric MC Works32 Version 3.00A (9.50.255.02); ICONICS GenBroker64, Platform Services, Workbench, FrameWorX Server v10.96 and prior; ICONICS GenBroker32 v9.5 and	https://us-cert.cisa.gov/ics/advisories/icsa-20-170-02, https://us-cert.cisa.gov/ics/advisories/icsa-20-170-03	A-MIT-MC_W-190820/378

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			prior. **CVE ID : CVE-2020-12009**		
Out-of-bounds Write	16-Jul-20	7.5	A specially crafted communication packet sent to the affected systems could cause a denial-of-service condition or allow remote code execution. This issue affects: Mitsubishi Electric MC Works64 version 4.02C (10.95.208.31) and earlier, all versions; MC Works32 version 3.00A (9.50.255.02); ICONICS GenBroker64, Platform Services, Workbench, FrameWorX Server version 10.96 and prior; GenBroker32 version 9.5 and prior. **CVE ID : CVE-2020-12011**	N/A	A-MIT-MC_W-190820/379
Improper Control of Generation of Code ('Code Injection')	16-Jul-20	6.4	A specially crafted WCF client that interfaces to the may allow the execution of certain arbitrary SQL commands remotely. This affects: Mitsubishi Electric MC Works64 Version 4.02C (10.95.208.31) and earlier, all versions; Mitsubishi Electric MC Works32 Version 3.00A (9.50.255.02); ICONICS GenBroker64, Platform Services, Workbench, FrameWorX Server v10.96 and prior; ICONICS GenBroker32 v9.5 and prior.	https://us-cert.cisa.gov/ics/advisories/icsa-20-170-02, https://us-cert.cisa.gov/ics/advisories/icsa-20-170-03	A-MIT-MC_W-190820/380

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2020-12013		
Deserialization of Untrusted Data	16-Jul-20	5	A specially crafted communication packet sent to the affected systems could cause a denial-of-service condition due to improper deserialization. This issue affects: Mitsubishi Electric MC Works64 version 4.02C (10.95.208.31) and earlier, all versions; Mitsubishi Electric MC Works32 version 3.00A (9.50.255.02); ICONICS GenBroker64, Platform Services, Workbench, FrameWorX Server version 10.96 and prior; ICONICS GenBroker32 version 9.5 and prior. **CVE ID : CVE-2020-12015**	https://www.us-cert.gov/ics/advisories/icsa-20-170-02, https://www.us-cert.gov/ics/advisories/icsa-20-170-03	A-MIT-MC_W-190820/381
mc_works32					
Deserialization of Untrusted Data	16-Jul-20	7.5	A specially crafted communication packet sent to the affected devices could allow remote code execution and a denial-of-service condition due to a deserialization vulnerability. This issue affects: Mitsubishi Electric MC Works64 version 4.02C (10.95.208.31) and earlier, all versions; Mitsubishi Electric MC Works32 version 3.00A (9.50.255.02); ICONICS GenBroker64, Platform Services, Workbench,	https://us-cert.cisa.gov/ics/advisories/icsa-20-170-02,, https://us-cert.cisa.gov/ics/advisories/icsa-20-170-03	A-MIT-MC_W-190820/382

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			FrameWorX Server version 10.96 and prior; ICONICS GenBroker32 version 9.5 and prior. **CVE ID : CVE-2020-12007**		
Deserialization of Untrusted Data	16-Jul-20	5	A specially crafted communication packet sent to the affected device could cause a denial-of-service condition due to a deserialization vulnerability. This affects: Mitsubishi Electric MC Works64 Version 4.02C (10.95.208.31) and earlier, all versions; Mitsubishi Electric MC Works32 Version 3.00A (9.50.255.02); ICONICS GenBroker64, Platform Services, Workbench, FrameWorX Server v10.96 and prior; ICONICS GenBroker32 v9.5 and prior. **CVE ID : CVE-2020-12009**	https://us-cert.cisa.gov/ics/advisories/icsa-20-170-02, https://us-cert.cisa.gov/ics/advisories/icsa-20-170-03	A-MIT-MC_W-190820/383
Out-of-bounds Write	16-Jul-20	7.5	A specially crafted communication packet sent to the affected systems could cause a denial-of-service condition or allow remote code execution. This issue affects: Mitsubishi Electric MC Works64 version 4.02C (10.95.208.31) and earlier, all versions; MC Works32 version 3.00A (9.50.255.02); ICONICS GenBroker64, Platform	N/A	A-MIT-MC_W-190820/384

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Services, Workbench, FrameWorX Server version 10.96 and prior; GenBroker32 version 9.5 and prior. **CVE ID : CVE-2020-12011**		
Improper Control of Generation of Code ('Code Injection')	16-Jul-20	6.4	A specially crafted WCF client that interfaces to the may allow the execution of certain arbitrary SQL commands remotely. This affects: Mitsubishi Electric MC Works64 Version 4.02C (10.95.208.31) and earlier, all versions; Mitsubishi Electric MC Works32 Version 3.00A (9.50.255.02); ICONICS GenBroker64, Platform Services, Workbench, FrameWorX Server v10.96 and prior; ICONICS GenBroker32 v9.5 and prior. **CVE ID : CVE-2020-12013**	https://us-cert.cisa.gov/ics/advisories/icsa-20-170-02, https://us-cert.cisa.gov/ics/advisories/icsa-20-170-03	A-MIT-MC_W-190820/385
Deserialization of Untrusted Data	16-Jul-20	5	A specially crafted communication packet sent to the affected systems could cause a denial-of-service condition due to improper deserialization. This issue affects: Mitsubishi Electric MC Works64 version 4.02C (10.95.208.31) and earlier, all versions; Mitsubishi Electric MC Works32 version 3.00A (9.50.255.02); ICONICS GenBroker64, Platform	https://www.us-cert.gov/ics/advisories/icsa-20-170-02, https://www.us-cert.gov/ics/advisories/icsa-20-170-03	A-MIT-MC_W-190820/386

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Services, Workbench, FrameWorX Server version 10.96 and prior; ICONICS GenBroker32 version 9.5 and prior. **CVE ID : CVE-2020-12015**		
mock2easy_project					
mock2easy					
Improper Neutralization of Special Elements in Output Used by a Downstream Component ('Injection')	29-Jul-20	7.5	This affects all versions of package mock2easy. a malicious user could inject commands through the _data variable: Affected Area require('../server/getJsonByCurl')(mock2easy, function (error, stdout) { if (error) { return res.json(500, error); } res.json(JSON.parse(stdout)); }, '', _data.interfaceUrl, query, _data.cookie,_data.interfaceType); **CVE ID : CVE-2020-7697**	N/A	A-MOC-MOCK-190820/387
mruby					
mruby					
Out-of-bounds Write	21-Jul-20	7.5	mruby through 2.1.2-rc has a heap-based buffer overflow in the mrb_yield_with_class function in vm.c because of incorrect VM stack handling. It can be triggered via the stack_copy function. **CVE ID : CVE-2020-15866**	N/A	A-MRU-MRUB-190820/388
munkireport_project					

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
munki_facts					
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	23-Jul-20	4.3	A Cross-Site Scripting (XSS) vulnerability in the munki_facts (aka Munki Conditions) module before 1.5 for MunkiReport allows remote attackers to inject arbitrary web script or HTML via the key name. **CVE ID : CVE-2020-15881**	N/A	A-MUN-MUNK-190820/389
managedinstalls					
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	23-Jul-20	4.3	A Cross-Site Scripting (XSS) vulnerability in the managedinstalls module before 2.6 for MunkiReport allows remote attackers to inject arbitrary web script or HTML via the last two URL parameters (through which installed packages names and versions are reported). **CVE ID : CVE-2020-15883**	N/A	A-MUN-MANA-190820/390
comment					
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	23-Jul-20	3.5	A Cross-Site Scripting (XSS) vulnerability in the comment module before 4.0 for MunkiReport allows remote attackers to inject arbitrary web script or HTML by posting a new comment. **CVE ID : CVE-2020-15885**	N/A	A-MUN-COMM-190820/391
reportdata					
Improper Neutralization of Special	23-Jul-20	6.5	A SQL injection vulnerability in reportdata_controller.php	N/A	A-MUN-REPO-190820/392

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Elements used in an SQL Command ('SQL Injection')			in the reportdata module before 3.5 for MunkiReport allows attackers to execute arbitrary SQL commands via the req parameter of the /module/reportdata/ip endpoint. **CVE ID : CVE-2020-15886**		
softwareupdate					
Improper Neutralization of Special Elements used in an SQL Command ('SQL Injection')	23-Jul-20	6.5	A SQL injection vulnerability in softwareupdate_controller.php in the Software Update module before 1.6 for MunkiReport allows attackers to execute arbitrary SQL commands via the last URL parameter of the /module/softwareupdate/get_tab_data/ endpoint. **CVE ID : CVE-2020-15887**	N/A	A-MUN-SOFT-190820/393
munkireport					
Cross-Site Request Forgery (CSRF)	23-Jul-20	5.8	A CSRF issue in manager/delete_machine/{id} in MunkiReport before 5.6.3 allows attackers to delete arbitrary machines from the MunkiReport database. **CVE ID : CVE-2020-15882**	N/A	A-MUN-MUNK-190820/394
Improper Neutralization of Special Elements used in an SQL	23-Jul-20	6.5	A SQL injection vulnerability in TableQuery.php in MunkiReport before 5.6.3 allows attackers to execute arbitrary SQL commands	N/A	A-MUN-MUNK-190820/395

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Command ('SQL Injection')			via the order[0][dir] field on POST requests to /datatables/data. **CVE ID : CVE-2020-15884**		
Nagios					
log_server					
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	30-Jul-20	3.5	A Stored XSS vulnerability exists in Nagios Log Server before 2.1.7 via the Notification Methods -> Email Users menu. **CVE ID : CVE-2020-16157**	N/A	A-NAG-LOG_-190820/396
nagios_xi					
N/A	22-Jul-20	7.5	In Nagios XI before 5.7.3, ajaxhelper.php allows remote authenticated attackers to execute arbitrary commands via cmdsubsys. **CVE ID : CVE-2020-15901**	N/A	A-NAG-NAGI-190820/397
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	22-Jul-20	4.3	Graph Explorer in Nagios XI before 5.7.2 allows XSS via the link url option. **CVE ID : CVE-2020-15902**	N/A	A-NAG-NAGI-190820/398
Ncp-e					
secure_enterprise_client					
Improper Link Resolution Before File Access ('Link	28-Jul-20	4.6	NCP Secure Enterprise Client before 10.15 r47589 allows a symbolic link attack on enumusb.reg via Support Assistant.	N/A	A-NCP-SECU-190820/399

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Following')			**CVE ID : CVE-2020-11474**		
NEC					
esmpro_manager					
Deserialization of Untrusted Data	22-Jul-20	7.5	This vulnerability allows remote attackers to execute arbitrary code on affected installations of NEC ESMPRO Manager 6.42. Authentication is not required to exploit this vulnerability. The specific flaw exists within the RMI service. The issue results from the lack of proper validation of user-supplied data, which can result in deserialization of untrusted data. An attacker can leverage this vulnerability to execute code in the context of SYSTEM. Was ZDI-CAN-10007. **CVE ID : CVE-2020-10917**	N/A	A-NEC-ESMP-190820/400
Nextcloud					
preferred_providers					
Improper Restriction of Excessive Authentication Attempts	30-Jul-20	5	Improper check of inputs in Nextcloud Preferred Providers app v1.6.0 allowed to perform a denial of service attack when using a very long password. **CVE ID : CVE-2020-8202**	N/A	A-NEX-PREF-190820/401
Nodejs					
node.js					
Improper Restriction	24-Jul-20	10	napi_get_value_string_*() allows various kinds of	N/A	A-NOD-NODE-

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
of Operations within the Bounds of a Memory Buffer			memory corruption in node < 10.21.0, 12.18.0, and < 14.4.0. **CVE ID : CVE-2020-8174**		190820/402
Octobercms					
october					
Reliance on Cookies without Validation and Integrity Checking	31-Jul-20	3.5	In OctoberCMS before version 1.0.468, encrypted cookie values were not tied to the name of the cookie the value belonged to. This meant that certain classes of attacks that took advantage of other theoretical vulnerabilities in user facing code (nothing exploitable in the core project itself) had a higher chance of succeeding. Specifically, if your usage exposed a way for users to provide unfiltered user input and have it returned to them as an encrypted cookie (ex. storing a user provided search query in a cookie) they could then use the generated cookie in place of other more tightly controlled cookies; or if your usage exposed the plaintext version of an encrypted cookie at any point to the user they could theoretically provide encrypted content from your application back to it	https://github.com/octobercms/october/security/advisories/GHSA-55mm-5399-7r63	A-OCT-OCTO-190820/403

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			as an encrypted cookie and force the framework to decrypt it for them. Issue has been fixed in build 468 (v1.0.468). **CVE ID : CVE-2020-15128**		
Openbsd					
openssh					
Improper Neutralization of Special Elements used in an OS Command ('OS Command Injection')	24-Jul-20	6.8	scp in OpenSSH through 8.3p1 allows command injection in scp.c remote function, as demonstrated by backtick characters in the destination argument. NOTE: the vendor reportedly has stated that they intentionally omit validation of "anomalous argument transfers" because that could "stand a great chance of breaking existing workflows." **CVE ID : CVE-2020-15778**	https://security.netapp.com/advisory/ntap-20200731-0007/	A-OPE-OPEN-190820/404
openclinic_ga_project					
openclinic_ga					
Improper Restriction of Excessive Authentication Attempts	20-Jul-20	5	OpenClinic GA versions 5.09.02 and 5.89.05b may allow an attacker to bypass the system's account lockout protection, which may allow brute force password attacks. **CVE ID : CVE-2020-14484**	N/A	A-OPE-OPEN-190820/405
Improper Authentication	20-Jul-20	7.5	OpenClinic GA versions 5.09.02 and 5.89.05b may allow an attacker to bypass client-side access	N/A	A-OPE-OPEN-190820/406

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			controls or use a crafted request to initiate a session with limited functionality, which may allow execution of admin functions such as SQL queries. **CVE ID : CVE-2020-14485**		
Incorrect Authorizatio n	29-Jul-20	6.5	An attacker may bypass permission/authorization checks in OpenClinic GA 5.09.02 and 5.89.05b by ignoring the redirect of a permission failure, which may allow unauthorized execution of commands. **CVE ID : CVE-2020-14486**	N/A	A-OPE-OPEN-190820/407
Insufficiently Protected Credentials	29-Jul-20	5	OpenClinic GA 5.09.02 and 5.89.05b stores passwords using inadequate hashing complexity, which may allow an attacker to recover passwords using known password cracking techniques. **CVE ID : CVE-2020-14489**	N/A	A-OPE-OPEN-190820/408
Improper Limitation of a Pathname to a Restricted Directory ('Path Traversal')	29-Jul-20	6.5	OpenClinic GA 5.09.02 and 5.89.05b includes arbitrary local files specified within its parameter and executes some files, which may allow disclosure of sensitive files or the execution of malicious uploaded files. **CVE ID : CVE-2020-14490**	N/A	A-OPE-OPEN-190820/409
Missing Authorizatio	20-Jul-20	4	OpenClinic GA versions 5.09.02 and 5.89.05b do	N/A	A-OPE-OPEN-

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
n			not properly check permissions before executing SQL queries, which may allow a low-privilege user to access privileged information. **CVE ID : CVE-2020-14491**		190820/410
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	29-Jul-20	4.3	OpenClinic GA 5.09.02 and 5.89.05b does not properly neutralize user-controllable input, which may allow the execution of malicious code within the user's browser. **CVE ID : CVE-2020-14492**	N/A	A-OPE-OPEN-190820/411
Improper Privilege Management	29-Jul-20	6.5	A low-privilege user may use SQL syntax to write arbitrary files to the OpenClinic GA 5.09.02 and 5.89.05b server, which may allow the execution of arbitrary commands. **CVE ID : CVE-2020-14493**	N/A	A-OPE-OPEN-190820/412
Improper Authentication	20-Jul-20	5	OpenClinic GA versions 5.09.02 and 5.89.05b contain an authentication mechanism within the system that does not provide sufficient complexity to protect against brute force attacks, which may allow unauthorized users to access the system after no more than a fixed maximum number of attempts. **CVE ID : CVE-2020-14494**	N/A	A-OPE-OPEN-190820/413

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Opennms					
opennms					
N/A	17-Jul-20	7.5	OpenNMS is accessible via port 9443 **CVE ID : CVE-2020-1652**	N/A	A-OPE-OPEN-190820/414
Opensuse					
backports_sle					
Information Exposure	22-Jul-20	4.3	Information leak in content security policy in Google Chrome prior to 84.0.4147.89 allowed a remote attacker to leak cross-origin data via a crafted HTML page. **CVE ID : CVE-2020-6511**	N/A	A-OPE-BACK-190820/415
Access of Resource Using Incompatible Type ('Type Confusion')	22-Jul-20	9.3	Type Confusion in V8 in Google Chrome prior to 84.0.4147.89 allowed a remote attacker to potentially exploit heap corruption via a crafted HTML page. **CVE ID : CVE-2020-6512**	N/A	A-OPE-BACK-190820/416
Improper Restriction of Operations within the Bounds of a Memory Buffer	22-Jul-20	6.8	Out of bounds memory access in developer tools in Google Chrome prior to 84.0.4147.89 allowed an attacker who convinced a user to install a malicious extension to potentially exploit heap corruption via a crafted Chrome Extension. **CVE ID : CVE-2020-6530**	N/A	A-OPE-BACK-190820/417
Access of Resource Using	22-Jul-20	6.8	Type Confusion in V8 in Google Chrome prior to 84.0.4147.89 allowed a	N/A	A-OPE-BACK-190820/418

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Incompatible Type ('Type Confusion')			remote attacker to potentially exploit heap corruption via a crafted HTML page. **CVE ID : CVE-2020-6533**		
Out-of-bounds Write	22-Jul-20	6.8	Heap buffer overflow in WebRTC in Google Chrome prior to 84.0.4147.89 allowed a remote attacker to potentially exploit heap corruption via a crafted HTML page. **CVE ID : CVE-2020-6534**	N/A	A-OPE-BACK-190820/419
Improper Input Validation	22-Jul-20	4.3	Insufficient data validation in WebUI in Google Chrome prior to 84.0.4147.89 allowed a remote attacker who had compromised the renderer process to inject scripts or HTML into a privileged page via a crafted HTML page. **CVE ID : CVE-2020-6535**	N/A	A-OPE-BACK-190820/420
Oracle					
mysql					
N/A	24-Jul-20	4	Vulnerability in the MySQL Server product of Oracle MySQL (component: Server: Optimizer). Supported versions that are affected are 8.0.20 and prior. Easily exploitable vulnerability allows high privileged attacker with network access via multiple protocols to compromise MySQL Server. Successful attacks	https://security.netapp.com/advisory/ntap-20200731-0006/	A-ORA-MYSQ-190820/421

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			of this vulnerability can result in unauthorized ability to cause a hang or frequently repeatable crash (complete DOS) of MySQL Server. CVSS 3.1 Base Score 4.9 (Availability impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:L/PR:H/UI:N/S:U/C:N/I:N/A:H). **CVE ID : CVE-2020-14725**		
Osisoft					
pi_data_archive					
NULL Pointer Dereference	24-Jul-20	4.9	An authenticated remote attacker could crash PI Archive Subsystem when the subsystem is working under memory pressure. This can result in blocking queries to PI Data Archive (2018 SP2 and prior versions). **CVE ID : CVE-2020-10600**	N/A	A-OSI-PI_D-190820/422
Improper Handling of Exceptional Conditions	25-Jul-20	5	In OSIsoft PI System multiple products and versions, a remote, unauthenticated attacker could crash PI Network Manager service through specially crafted requests. This can result in blocking connections and queries to PI Data Archive. **CVE ID : CVE-2020-10604**	N/A	A-OSI-PI_D-190820/423
Incorrect Default Permissions	24-Jul-20	4.6	In OSIsoft PI System multiple products and versions, a local attacker can exploit incorrect	N/A	A-OSI-PI_D-190820/424

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			permissions set by affected PI System software. This exploitation can result in unauthorized information disclosure, deletion, or modification if the local computer also processes PI System data from other users, such as from a shared workstation or terminal server deployment. **CVE ID : CVE-2020-10606**		
Improper Verification of Cryptographic Signature	24-Jul-20	4.6	In OSIsoft PI System multiple products and versions, a local attacker can plant a binary and bypass a code integrity check for loading PI System libraries. This exploitation can target another local user of PI System software on the computer to escalate privilege and result in unauthorized information disclosure, deletion, or modification. **CVE ID : CVE-2020-10608**	N/A	A-OSI-PI_D-190820/425
Uncontrolled Search Path Element	24-Jul-20	7.2	In OSIsoft PI System multiple products and versions, a local attacker can modify a search path and plant a binary to exploit the affected PI System software to take control of the local computer at Windows system privilege level, resulting in unauthorized	N/A	A-OSI-PI_D-190820/426

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			information disclosure, deletion, or modification. **CVE ID : CVE-2020-10610**		
pi_api					
Incorrect Default Permissions	24-Jul-20	4.6	In OSIsoft PI System multiple products and versions, a local attacker can exploit incorrect permissions set by affected PI System software. This exploitation can result in unauthorized information disclosure, deletion, or modification if the local computer also processes PI System data from other users, such as from a shared workstation or terminal server deployment. **CVE ID : CVE-2020-10606**	N/A	A-OSI-PI_A-190820/427
Improper Verification of Cryptographic Signature	24-Jul-20	4.6	In OSIsoft PI System multiple products and versions, a local attacker can plant a binary and bypass a code integrity check for loading PI System libraries. This exploitation can target another local user of PI System software on the computer to escalate privilege and result in unauthorized information disclosure, deletion, or modification. **CVE ID : CVE-2020-10608**	N/A	A-OSI-PI_A-190820/428
Uncontrolled Search Path	24-Jul-20	7.2	In OSIsoft PI System multiple products and	N/A	A-OSI-PI_A-190820/429

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Element			versions, a local attacker can modify a search path and plant a binary to exploit the affected PI System software to take control of the local computer at Windows system privilege level, resulting in unauthorized information disclosure, deletion, or modification. **CVE ID : CVE-2020-10610**		
pi_buffer_subsystem					
Incorrect Default Permissions	24-Jul-20	4.6	In OSIsoft PI System multiple products and versions, a local attacker can exploit incorrect permissions set by affected PI System software. This exploitation can result in unauthorized information disclosure, deletion, or modification if the local computer also processes PI System data from other users, such as from a shared workstation or terminal server deployment. **CVE ID : CVE-2020-10606**	N/A	A-OSI-PI_B-190820/430
Improper Verification of Cryptographic Signature	24-Jul-20	4.6	In OSIsoft PI System multiple products and versions, a local attacker can plant a binary and bypass a code integrity check for loading PI System libraries. This exploitation can target another local user of PI System software on the	N/A	A-OSI-PI_B-190820/431

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			computer to escalate privilege and result in unauthorized information disclosure, deletion, or modification. **CVE ID : CVE-2020-10608**		
Uncontrolled Search Path Element	24-Jul-20	7.2	In OSIsoft PI System multiple products and versions, a local attacker can modify a search path and plant a binary to exploit the affected PI System software to take control of the local computer at Windows system privilege level, resulting in unauthorized information disclosure, deletion, or modification. **CVE ID : CVE-2020-10610**	N/A	A-OSI-PI_B-190820/432
pi_connector					
Incorrect Default Permissions	24-Jul-20	4.6	In OSIsoft PI System multiple products and versions, a local attacker can exploit incorrect permissions set by affected PI System software. This exploitation can result in unauthorized information disclosure, deletion, or modification if the local computer also processes PI System data from other users, such as from a shared workstation or terminal server deployment. **CVE ID : CVE-2020-10606**	N/A	A-OSI-PI_C-190820/433
Improper	24-Jul-20	4.6	In OSIsoft PI System	N/A	A-OSI-PI_C-

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Verification of Cryptographic Signature			multiple products and versions, a local attacker can plant a binary and bypass a code integrity check for loading PI System libraries. This exploitation can target another local user of PI System software on the computer to escalate privilege and result in unauthorized information disclosure, deletion, or modification. **CVE ID : CVE-2020-10608**		190820/434
Uncontrolled Search Path Element	24-Jul-20	7.2	In OSIsoft PI System multiple products and versions, a local attacker can modify a search path and plant a binary to exploit the affected PI System software to take control of the local computer at Windows system privilege level, resulting in unauthorized information disclosure, deletion, or modification. **CVE ID : CVE-2020-10610**	N/A	A-OSI-PI_C-190820/435
pi_connector_relay					
Incorrect Default Permissions	24-Jul-20	4.6	In OSIsoft PI System multiple products and versions, a local attacker can exploit incorrect permissions set by affected PI System software. This exploitation can result in unauthorized information disclosure, deletion, or modification if the local	N/A	A-OSI-PI_C-190820/436

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			computer also processes PI System data from other users, such as from a shared workstation or terminal server deployment. **CVE ID : CVE-2020-10606**		
Improper Verification of Cryptographic Signature	24-Jul-20	4.6	In OSIsoft PI System multiple products and versions, a local attacker can plant a binary and bypass a code integrity check for loading PI System libraries. This exploitation can target another local user of PI System software on the computer to escalate privilege and result in unauthorized information disclosure, deletion, or modification. **CVE ID : CVE-2020-10608**	N/A	A-OSI-PI_C-190820/437
Uncontrolled Search Path Element	24-Jul-20	7.2	In OSIsoft PI System multiple products and versions, a local attacker can modify a search path and plant a binary to exploit the affected PI System software to take control of the local computer at Windows system privilege level, resulting in unauthorized information disclosure, deletion, or modification. **CVE ID : CVE-2020-10610**	N/A	A-OSI-PI_C-190820/438
pi_data_collection_manager					
Incorrect	24-Jul-20	4.6	In OSIsoft PI System	N/A	A-OSI-PI_D-

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Default Permissions			multiple products and versions, a local attacker can exploit incorrect permissions set by affected PI System software. This exploitation can result in unauthorized information disclosure, deletion, or modification if the local computer also processes PI System data from other users, such as from a shared workstation or terminal server deployment. **CVE ID : CVE-2020-10606**		190820/439
Improper Verification of Cryptographic Signature	24-Jul-20	4.6	In OSIsoft PI System multiple products and versions, a local attacker can plant a binary and bypass a code integrity check for loading PI System libraries. This exploitation can target another local user of PI System software on the computer to escalate privilege and result in unauthorized information disclosure, deletion, or modification. **CVE ID : CVE-2020-10608**	N/A	A-OSI-PI_D-190820/440
Uncontrolled Search Path Element	24-Jul-20	7.2	In OSIsoft PI System multiple products and versions, a local attacker can modify a search path and plant a binary to exploit the affected PI System software to take control of the local	N/A	A-OSI-PI_D-190820/441

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			computer at Windows system privilege level, resulting in unauthorized information disclosure, deletion, or modification. **CVE ID : CVE-2020-10610**		
pi_integrator					
Incorrect Default Permissions	24-Jul-20	4.6	In OSIsoft PI System multiple products and versions, a local attacker can exploit incorrect permissions set by affected PI System software. This exploitation can result in unauthorized information disclosure, deletion, or modification if the local computer also processes PI System data from other users, such as from a shared workstation or terminal server deployment. **CVE ID : CVE-2020-10606**	N/A	A-OSI-PI_I-190820/442
Improper Verification of Cryptographic Signature	24-Jul-20	4.6	In OSIsoft PI System multiple products and versions, a local attacker can plant a binary and bypass a code integrity check for loading PI System libraries. This exploitation can target another local user of PI System software on the computer to escalate privilege and result in unauthorized information disclosure, deletion, or modification.	N/A	A-OSI-PI_I-190820/443

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2020-10608		
Uncontrolled Search Path Element	24-Jul-20	7.2	In OSIsoft PI System multiple products and versions, a local attacker can modify a search path and plant a binary to exploit the affected PI System software to take control of the local computer at Windows system privilege level, resulting in unauthorized information disclosure, deletion, or modification. **CVE ID : CVE-2020-10610**	N/A	A-OSI-PI_I-190820/444
pi_interface_configuration_utility					
Incorrect Default Permissions	24-Jul-20	4.6	In OSIsoft PI System multiple products and versions, a local attacker can exploit incorrect permissions set by affected PI System software. This exploitation can result in unauthorized information disclosure, deletion, or modification if the local computer also processes PI System data from other users, such as from a shared workstation or terminal server deployment. **CVE ID : CVE-2020-10606**	N/A	A-OSI-PI_I-190820/445
Improper Verification of Cryptographic Signature	24-Jul-20	4.6	In OSIsoft PI System multiple products and versions, a local attacker can plant a binary and bypass a code integrity check for loading PI	N/A	A-OSI-PI_I-190820/446

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			System libraries. This exploitation can target another local user of PI System software on the computer to escalate privilege and result in unauthorized information disclosure, deletion, or modification. **CVE ID : CVE-2020-10608**		
Uncontrolled Search Path Element	24-Jul-20	7.2	In OSIsoft PI System multiple products and versions, a local attacker can modify a search path and plant a binary to exploit the affected PI System software to take control of the local computer at Windows system privilege level, resulting in unauthorized information disclosure, deletion, or modification. **CVE ID : CVE-2020-10610**	N/A	A-OSI-PI_I-190820/447
pi_to_ocs					
Incorrect Default Permissions	24-Jul-20	4.6	In OSIsoft PI System multiple products and versions, a local attacker can exploit incorrect permissions set by affected PI System software. This exploitation can result in unauthorized information disclosure, deletion, or modification if the local computer also processes PI System data from other users, such as from a shared workstation or terminal server	N/A	A-OSI-PI_T-190820/448

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			deployment. **CVE ID : CVE-2020-10606**		
Improper Verification of Cryptographic Signature	24-Jul-20	4.6	In OSIsoft PI System multiple products and versions, a local attacker can plant a binary and bypass a code integrity check for loading PI System libraries. This exploitation can target another local user of PI System software on the computer to escalate privilege and result in unauthorized information disclosure, deletion, or modification. **CVE ID : CVE-2020-10608**	N/A	A-OSI-PI_T-190820/449
Uncontrolled Search Path Element	24-Jul-20	7.2	In OSIsoft PI System multiple products and versions, a local attacker can modify a search path and plant a binary to exploit the affected PI System software to take control of the local computer at Windows system privilege level, resulting in unauthorized information disclosure, deletion, or modification. **CVE ID : CVE-2020-10610**	N/A	A-OSI-PI_T-190820/450
pi_vision					
Improper Neutralization of Input During Web Page Generation	25-Jul-20	3.5	In OSIsoft PI System multiple products and versions, an authenticated remote attacker with write access to PI Vision databases could inject	N/A	A-OSI-PI_V-190820/451

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
('Cross-site Scripting')			code into a display. Unauthorized information disclosure, deletion, or modification is possible if a victim views the infected display. **CVE ID : CVE-2020-10614**		
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	27-Jul-20	3.5	An authenticated remote attacker could use specially crafted URLs to send a victim using PI Vision 2019 mobile to a vulnerable web page due to a known issue in a third-party component. **CVE ID : CVE-2020-10643**	N/A	A-OSI-PI_V-190820/452
Otrs					
otrs					
Insufficient Session Expiration	20-Jul-20	4	When an agent user is renamed or set to invalid the session belonging to the user is keept active. The session can not be used to access ticket data in the case the agent is invalid. This issue affects ((OTRS)) Community Edition: 6.0.28 and prior versions. OTRS: 7.0.18 and prior versions, 8.0.4. and prior versions. **CVE ID : CVE-2020-1776**	https://otrs.com/release-notes/otrs-security-advisory-2020-13/	A-OTR-OTRS-190820/453
overwolf					
overwolf					
Improper Link Resolution Before File	24-Jul-20	9	Overwolf before 0.149.2.30 mishandles Symbolic Links during updates, causing elevation	N/A	A-OVE-OVER-190820/454

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Access ('Link Following')			of privileges. **CVE ID : CVE-2020-15932**		
Parallels					
remote_application_server					
N/A	24-Jul-20	6.5	Parallels Remote Application Server (RAS) 17.1.1 has a Business Logic Error causing remote code execution. It allows an authenticated user to execute any application in the backend operating system through the web application, despite the affected application not being published. In addition, it was discovered that it is possible to access any host in the internal domain, even if it has no published applications or the mentioned host is no longer associated with that server farm. **CVE ID : CVE-2020-15860**	N/A	A-PAR-REMO-190820/455
parseplatform					
parse_server					
Incorrect Authorization	22-Jul-20	4	In parser-server from version 3.5.0 and before 4.3.0, an authenticated user using the viewer GraphQL query can by pass all read security on his User object and can also by pass all objects linked via relation or Pointer on his User object. **CVE ID : CVE-2020-15126**	https://github.com/parse-community/parse-server/security/advisories/GHSA-236h-rqv8-8q73	A-PAR-PARS-190820/456

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Phoenixcontact					
plcnext_engineer					
Improper Limitation of a Pathname to a Restricted Directory ('Path Traversal')	21-Jul-20	4.4	In PHOENIX CONTACT PLCnext Engineer version 2020.3.1 and earlier an improper path sanitation vulnerability exists on import of project files. **CVE ID : CVE-2020-12499**	https://cert.vde.com/en-us/advisories/vde-2020-025	A-PHO-PLCN-190820/457
pi					
data_archive					
NULL Pointer Dereference	24-Jul-20	3.5	In OSIsoft PI System multiple products and versions, an authenticated remote attacker could crash PI Network Manager due to a race condition. This can result in blocking connections and queries to PI Data Archive. **CVE ID : CVE-2020-10602**	N/A	A-PI-DATA-190820/458
pi-hole					
pi-hole					
Improper Privilege Management	30-Jul-20	7.2	An issue was discovered in Pi-Hole through 5.0. The local www-data user has sudo privileges to execute the pihole core script as root without a password, which could allow an attacker to obtain root access via shell metacharacters to this script's setdns command. **CVE ID : CVE-2020-14162**	N/A	A-PI--PI-H-190820/459
Improper Privilege	30-Jul-20	7.2	Pi-hole 4.4 allows a user able to write to	N/A	A-PI--PI-H-

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Management			/etc/pihole/dns-servers.conf to escalate privileges through command injection (shell metacharacters after an IP address). **CVE ID : CVE-2020-12620**		190820/460
Prestashop					
dashboard_products					
Incorrect Authorization	21-Jul-20	4	In PrestaShop Dashboard Productions before version 2.1.0, there is improper authorization which enables an attacker to change the configuration. The problem is fixed in 2.1.0. **CVE ID : CVE-2020-15102**	https://github.com/PrestaShop/dashproducts/security/advisories/GHSA-6292-4qpg-hvfg	A-PRE-DASH-190820/461
Pulsesecure					
pulse_policy_secure					
Information Exposure	27-Jul-20	2.1	An issue was discovered in Pulse Policy Secure (PPS) and Pulse Connect Secure (PCS) Virtual Appliance before 9.1R8. By manipulating a certain kernel boot parameter, it can be tricked into dropping into a root shell in a pre-install phase where the entire source code of the appliance is available and can be retrieved. (The source code is otherwise inaccessible because the appliance has its hard disks encrypted, and no root shell is available	https://kb.pulsesecure.net/articles/Pulse_Security_Advisories/SA44516	A-PUL-PULS-190820/462

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			during normal operation.) **CVE ID : CVE-2020-12880**		
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	30-Jul-20	4.3	A cross site scripting (XSS) vulnerability exists in Pulse Connect Secure <9.1R5 on the PSAL Page. **CVE ID : CVE-2020-8204**	N/A	A-PUL-PULS-190820/463
Improper Authentication	30-Jul-20	7.5	An improper authentication vulnerability exists in Pulse Connect Secure <9.1RB that allows an attacker with a users primary credentials to bypass the Google TOTP. **CVE ID : CVE-2020-8206**	N/A	A-PUL-PULS-190820/464
Information Exposure	30-Jul-20	4	An information disclosure vulnerability in meeting of Pulse Connect Secure <9.1R8 allowed an authenticated end-users to find meeting details, if they know the Meeting ID. **CVE ID : CVE-2020-8216**	N/A	A-PUL-PULS-190820/465
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	30-Jul-20	3.5	A cross site scripting (XSS) vulnerability in Pulse Connect Secure <9.1R8 allowed attackers to exploit in the URL used for Citrix ICA. **CVE ID : CVE-2020-8217**	N/A	A-PUL-PULS-190820/466
Improper Control of Generation of Code	30-Jul-20	6.5	A code injection vulnerability exists in Pulse Connect Secure <9.1RB that allows an	N/A	A-PUL-PULS-190820/467

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
('Code Injection')			attacker to crafted a URI to perform an arbitrary code execution via the admin web interface. **CVE ID : CVE-2020-8218**		
Incorrect Default Permissions	30-Jul-20	4	An insufficient permission check vulnerability exists in Pulse Connect Secure <9.1R8 that allows an attacker to change the password of a full administrator. **CVE ID : CVE-2020-8219**	N/A	A-PUL-PULS-190820/468
Uncontrolled Resource Consumption	30-Jul-20	5.5	A denial of service vulnerability exists in Pulse Connect Secure <9.1R8 that allows an authenticated attacker to perform command injection via the administrator web which can cause DOS. **CVE ID : CVE-2020-8220**	N/A	A-PUL-PULS-190820/469
Improper Limitation of a Pathname to a Restricted Directory ('Path Traversal')	30-Jul-20	4	A path traversal vulnerability exists in Pulse Connect Secure <9.1R8 which allows an authenticated attacker to read arbitrary files via the administrator web interface. **CVE ID : CVE-2020-8221**	N/A	A-PUL-PULS-190820/470
Improper Limitation of a Pathname to a Restricted Directory ('Path	30-Jul-20	4	A path traversal vulnerability exists in Pulse Connect Secure <9.1R8 that allowed an authenticated attacker via the administrator web interface to perform an	N/A	A-PUL-PULS-190820/471

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Traversal')			arbitrary file reading vulnerability through Meeting. **CVE ID : CVE-2020-8222**		
pulse_connect_secure					
Information Exposure	27-Jul-20	2.1	An issue was discovered in Pulse Policy Secure (PPS) and Pulse Connect Secure (PCS) Virtual Appliance before 9.1R8. By manipulating a certain kernel boot parameter, it can be tricked into dropping into a root shell in a pre-install phase where the entire source code of the appliance is available and can be retrieved. (The source code is otherwise inaccessible because the appliance has its hard disks encrypted, and no root shell is available during normal operation.) **CVE ID : CVE-2020-12880**	https://kb.pulsesecure.net/articles/Pulse_Security_Advisories/SA44516	A-PUL-PULS-190820/472
Missing Authorization	28-Jul-20	5.8	An issue was discovered in Pulse Secure Pulse Connect Secure before 9.1R8. An authenticated attacker can access the admin page console via the end-user web interface because of a rewrite. **CVE ID : CVE-2020-15408**	https://kb.pulsesecure.net/articles/Pulse_Security_Advisories/SA44516	A-PUL-PULS-190820/473
Improper Neutralization of Input During Web	30-Jul-20	4.3	A cross site scripting (XSS) vulnerability exists in Pulse Connect Secure <9.1R5 on the PSAL Page.	N/A	A-PUL-PULS-190820/474

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Page Generation ('Cross-site Scripting')			**CVE ID : CVE-2020-8204**		
Improper Authenticati on	30-Jul-20	7.5	An improper authentication vulnerability exists in Pulse Connect Secure <9.1RB that allows an attacker with a users primary credentials to bypass the Google TOTP. **CVE ID : CVE-2020-8206**	N/A	A-PUL-PULS-190820/475
Information Exposure	30-Jul-20	4	An information disclosure vulnerability in meeting of Pulse Connect Secure <9.1R8 allowed an authenticated end-users to find meeting details, if they know the Meeting ID. **CVE ID : CVE-2020-8216**	N/A	A-PUL-PULS-190820/476
Improper Neutralizatio n of Input During Web Page Generation ('Cross-site Scripting')	30-Jul-20	3.5	A cross site scripting (XSS) vulnerability in Pulse Connect Secure <9.1R8 allowed attackers to exploit in the URL used for Citrix ICA. **CVE ID : CVE-2020-8217**	N/A	A-PUL-PULS-190820/477
Improper Control of Generation of Code ('Code Injection')	30-Jul-20	6.5	A code injection vulnerability exists in Pulse Connect Secure <9.1RB that allows an attacker to crafted a URI to perform an arbitrary code execution via the admin web interface. **CVE ID : CVE-2020-8218**	N/A	A-PUL-PULS-190820/478

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Incorrect Default Permissions	30-Jul-20	4	An insufficient permission check vulnerability exists in Pulse Connect Secure <9.1R8 that allows an attacker to change the password of a full administrator. **CVE ID : CVE-2020-8219**	N/A	A-PUL-PULS-190820/479
Uncontrolled Resource Consumption	30-Jul-20	5.5	A denial of service vulnerability exists in Pulse Connect Secure <9.1R8 that allows an authenticated attacker to perform command injection via the administrator web which can cause DOS. **CVE ID : CVE-2020-8220**	N/A	A-PUL-PULS-190820/480
Improper Limitation of a Pathname to a Restricted Directory ('Path Traversal')	30-Jul-20	4	A path traversal vulnerability exists in Pulse Connect Secure <9.1R8 which allows an authenticated attacker to read arbitrary files via the administrator web interface. **CVE ID : CVE-2020-8221**	N/A	A-PUL-PULS-190820/481
Improper Limitation of a Pathname to a Restricted Directory ('Path Traversal')	30-Jul-20	4	A path traversal vulnerability exists in Pulse Connect Secure <9.1R8 that allowed an authenticated attacker via the administrator web interface to perform an arbitrary file reading vulnerability through Meeting. **CVE ID : CVE-2020-8222**	N/A	A-PUL-PULS-190820/482

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
pulse_secure_desktop_client					
Missing Authorization	28-Jul-20	5.8	An issue was discovered in Pulse Secure Pulse Connect Secure before 9.1R8. An authenticated attacker can access the admin page console via the end-user web interface because of a rewrite. **CVE ID : CVE-2020-15408**	https://kb.pulsesecure.net/articles/Pulse_Security_Advisories/SA44516	A-PUL-PULS-190820/483
pypi					
bsdiff4					
Out-of-bounds Write	22-Jul-20	6.8	A buffer overflow in the patching routine of bsdiff4 before 1.2.0 allows an attacker to write to heap memory (beyond allocated bounds) via a crafted patch file. **CVE ID : CVE-2020-15904**	N/A	A-PYP-BSDI-190820/484
Python					
python					
Incorrect Authorization	17-Jul-20	7.5	In Python 3.8.4, sys.path restrictions specified in a python38._pth file are ignored, allowing code to be loaded from arbitrary locations. The <executable-name>._pth file (e.g., the python._pth file) is not affected. **CVE ID : CVE-2020-15801**	https://security.netapp.com/advisory/ntap-20200731-0003/	A-PYT-PYTH-190820/485
Qemu					
qemu					
Use After Free	21-Jul-20	2.1	QEMU 4.2.0 has a use-after-free in hw/net/e1000e_core.c	N/A	A-QEM-QEMU-190820/486

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			because a guest OS user can trigger an e1000e packet with the data's address set to the e1000e's MMIO address. **CVE ID : CVE-2020-15859**		
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	28-Jul-20	7.2	hw/net/xgmac.c in the XGMAC Ethernet controller in QEMU before 07-20-2020 has a buffer overflow. This occurs during packet transmission and affects the highbank and midway emulated machines. A guest user or process could use this flaw to crash the QEMU process on the host, resulting in a denial of service or potential privileged code execution. This was fixed in commit 5519724a13664b43e225ca05351c60b4468e4555. **CVE ID : CVE-2020-15863**	http://www.openwall.com/lists/oss-security/2020/07/22/1, https://git.qemu.org/?p=qemu.git;a=commitdiff;h=5519724a13664b43e225ca05351c60b4468e4555	A-QEM-QEMU-190820/487
Radare					
radare2					
Improper Neutralization of Special Elements used in an OS Command ('OS Command Injection')	20-Jul-20	6.8	In radare2 before version 4.5.0, malformed PDB file names in the PDB server path cause shell injection. To trigger the problem it's required to open the executable in radare2 and run idpd to trigger the download. The shell code will execute, and will create a file called pwned in the current directory.	https://github.com/radareorg/radare2/security/advisories/GHSA-r552-vp94-9358	A-RAD-RADA-190820/488

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2020-15121		
raspberrytorte					
raspberrytortoise					
Improper Neutralization of Special Elements in Output Used by a Downstream Component ('Injection')	23-Jul-20	10	The WebControl in RaspberryTortoise through 2012-10-28 is vulnerable to remote code execution via shell metacharacters in a URI. The file nodejs/raspberryTortoise.js has no validation on the parameter incomingString before passing it to the child_process.exec function. **CVE ID : CVE-2020-15477**	N/A	A-RAS-RASP-190820/489
rconfig					
rconfig					
Improper Limitation of a Pathname to a Restricted Directory ('Path Traversal')	28-Jul-20	4	rConfig 3.9.5 could allow a remote authenticated attacker to traverse directories on the system. An attacker could send a crafted request to the ajaxGetFileByPath.php script containing hexadecimal encoded "dot dot" sequences (%2f..%2f) in the path parameter to view arbitrary files on the system. **CVE ID : CVE-2020-15712**	N/A	A-RCO-RCON-190820/490
Improper Neutralization of Special Elements used in an	28-Jul-20	6.5	rConfig 3.9.5 is vulnerable to SQL injection. A remote authenticated attacker could send crafted SQL statements to the	N/A	A-RCO-RCON-190820/491

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
SQL Command ('SQL Injection')			devices.php script using the sortBy parameter, which could allow the attacker to view, add, modify, or delete information in the back-end database. **CVE ID : CVE-2020-15713**		
Improper Neutralization of Special Elements used in an SQL Command ('SQL Injection')	28-Jul-20	6.5	rConfig 3.9.5 is vulnerable to SQL injection. A remote authenticated attacker could send crafted SQL statements to the devices.crud.php script using the custom_Location parameter, which could allow the attacker to view, add, modify, or delete information in the back-end database. **CVE ID : CVE-2020-15714**	N/A	A-RCO-RCON-190820/492
N/A	28-Jul-20	6.5	rConfig 3.9.5 could allow a remote authenticated attacker to execute arbitrary code on the system, because of an error in the search.crud.php script. An attacker could exploit this vulnerability using the nodeId parameter. **CVE ID : CVE-2020-15715**	N/A	A-RCO-RCON-190820/493
react-native-fast-image_project					
react-native-fast-image					
Information Exposure	17-Jul-20	5	This affects all versions of package react-native-fast-image. When an image with source={{uri: "...", headers: { host:	N/A	A-REA-REAC-190820/494

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			"somehost.com", authorization: "..." }} is loaded, all other subsequent images will use the same headers, this can lead to signing credentials or other session tokens being leaked to other servers. **CVE ID : CVE-2020-7696**		
Redhat					
openshift_application_runtimes					
Uncontrolled Resource Consumption	24-Jul-20	4	A vulnerability was found in Wildfly's Enterprise Java Beans (EJB) versions shipped with Red Hat JBoss EAP 7, where SessionOpenInvocations are never removed from the remote InvocationTracker after a response is received in the EJB Client, as well as the server. This flaw allows an attacker to craft a denial of service attack to make the service unavailable. **CVE ID : CVE-2020-14307**	https://bugzilla.redhat.com/show_bug.cgi?id=CVE-2020-14307	A-RED-OPEN-190820/495
Uncontrolled Resource Consumption	24-Jul-20	4	A flaw was discovered in Wildfly's EJB Client as shipped with Red Hat JBoss EAP 7, where some specific EJB transaction objects may get accumulated over the time and can cause services to slow down and eventaully unavailable. An attacker can take advantage and	https://bugzilla.redhat.com/show_bug.cgi?id=CVE-2020-14297	A-RED-OPEN-190820/496

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			cause denial of service attack and make services unavailable. **CVE ID : CVE-2020-14297**		
jboss_fuse					
Uncontrolled Resource Consumption	24-Jul-20	4	A flaw was discovered in Wildfly's EJB Client as shipped with Red Hat JBoss EAP 7, where some specific EJB transaction objects may get accumulated over the time and can cause services to slow down and eventaully unavailable. An attacker can take advantage and cause denial of service attack and make services unavailable. **CVE ID : CVE-2020-14297**	https://bugzilla.redhat.com/show_bug.cgi?id=CVE-2020-14297	A-RED-JBOS-190820/497
Uncontrolled Resource Consumption	24-Jul-20	4	A vulnerability was found in Wildfly's Enterprise Java Beans (EJB) versions shipped with Red Hat JBoss EAP 7, where SessionOpenInvocations are never removed from the remote InvocationTracker after a response is received in the EJB Client, as well as the server. This flaw allows an attacker to craft a denial of service attack to make the service unavailable. **CVE ID : CVE-2020-14307**	https://bugzilla.redhat.com/show_bug.cgi?id=CVE-2020-14307	A-RED-JBOS-190820/498
openstack_platform					
Improper Privilege	31-Jul-20	6.5	A flaw was found in the nova_libvirt container	N/A	A-RED-OPEN-

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Management			provided by the Red Hat OpenStack Platform 16, where it does not have SELinux enabled. This flaw causes sVirt, an important isolation mechanism, to be disabled for all running virtual machines. **CVE ID : CVE-2020-10731**		190820/499
enterprise_linux_atomic_host					
Improper Verification of Cryptographic Signature	29-Jul-20	4.4	GRUB2 fails to validate kernel signature when booted directly without shim, allowing secure boot to be bypassed. This only affects systems where the kernel signing certificate has been imported directly into the secure boot database and the GRUB image is booted directly without the use of shim. This issue affects GRUB2 version 2.04 and prior versions. **CVE ID : CVE-2020-15705**	https://lists.gnu.org/archive/html/grub-devel/2020-07/msg00034.html, https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/ADV200011, https://security.netapp.com/advisory/ntap-20200731-0008/	A-RED-ENTE-190820/500
Concurrent Execution using Shared Resource with Improper Synchronization ('Race Condition')	29-Jul-20	4.4	GRUB2 contains a race condition in grub_script_function_create() leading to a use-after-free vulnerability which can be triggered by redefining a function whilst the same function is already executing, leading to arbitrary code execution	https://lists.gnu.org/archive/html/grub-devel/2020-07/msg00034.html, https://portal.msrc.microsoft.com/en	A-RED-ENTE-190820/501

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			and secure boot restriction bypass. This issue affects GRUB2 version 2.04 and prior versions. **CVE ID : CVE-2020-15706**	-US/security-guidance/advisory/ADV200011, https://security.netapp.com/advisory/ntap-20200731-0008/	
Concurrent Execution using Shared Resource with Improper Synchronization ('Race Condition')	29-Jul-20	4.4	Integer overflows were discovered in the functions grub_cmd_initrd and grub_initrd_init in the efilinux component of GRUB2, as shipped in Debian, Red Hat, and Ubuntu (the functionality is not included in GRUB2 upstream), leading to a heap-based buffer overflow. These could be triggered by an extremely large number of arguments to the initrd command on 32-bit architectures, or a crafted filesystem with very large files on any architecture. An attacker could use this to execute arbitrary code and bypass UEFI Secure Boot restrictions. This issue affects GRUB2 version 2.04 and prior versions. **CVE ID : CVE-2020-15707**	https://lists.gnu.org/archive/html/grub-devel/2020-07/msg00034.html, https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/ADV200011, https://security.netapp.com/advisory/ntap-20200731-0008/	A-RED-ENTE-190820/502
single_sign-on					
Uncontrolled Resource	24-Jul-20	4	A vulnerability was found in Wildfly's Enterprise Java	https://bugzilla.redhat.co	A-RED-SING-190820/503

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Consumption			Beans (EJB) versions shipped with Red Hat JBoss EAP 7, where SessionOpenInvocations are never removed from the remote InvocationTracker after a response is received in the EJB Client, as well as the server. This flaw allows an attacker to craft a denial of service attack to make the service unavailable. **CVE ID : CVE-2020-14307**	m/show_bug.cgi?id=CVE-2020-14307	
Uncontrolled Resource Consumption	24-Jul-20	4	A flaw was discovered in Wildfly's EJB Client as shipped with Red Hat JBoss EAP 7, where some specific EJB transaction objects may get accumulated over the time and can cause services to slow down and eventaully unavailable. An attacker can take advantage and cause denial of service attack and make services unavailable. **CVE ID : CVE-2020-14297**	https://bugzilla.redhat.com/show_bug.cgi?id=CVE-2020-14297	A-RED-SING-190820/504
jboss_enterprise_application_platform_continuous_delivery					
Uncontrolled Resource Consumption	24-Jul-20	4	A vulnerability was found in Wildfly's Enterprise Java Beans (EJB) versions shipped with Red Hat JBoss EAP 7, where SessionOpenInvocations are never removed from the remote InvocationTracker after a response is received in the	https://bugzilla.redhat.com/show_bug.cgi?id=CVE-2020-14307	A-RED-JBOS-190820/505

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			EJB Client, as well as the server. This flaw allows an attacker to craft a denial of service attack to make the service unavailable. **CVE ID : CVE-2020-14307**		
Uncontrolled Resource Consumption	24-Jul-20	4	A flaw was discovered in Wildfly's EJB Client as shipped with Red Hat JBoss EAP 7, where some specific EJB transaction objects may get accumulated over the time and can cause services to slow down and eventaully unavailable. An attacker can take advantage and cause denial of service attack and make services unavailable. **CVE ID : CVE-2020-14297**	https://bugzilla.redhat.com/show_bug.cgi?id=CVE-2020-14297	A-RED-JBOS-190820/506
amq					
Uncontrolled Resource Consumption	24-Jul-20	4	A vulnerability was found in Wildfly's Enterprise Java Beans (EJB) versions shipped with Red Hat JBoss EAP 7, where SessionOpenInvocations are never removed from the remote InvocationTracker after a response is received in the EJB Client, as well as the server. This flaw allows an attacker to craft a denial of service attack to make the service unavailable. **CVE ID : CVE-2020-14307**	https://bugzilla.redhat.com/show_bug.cgi?id=CVE-2020-14307	A-RED-AMQ-190820/507
Uncontrolled	24-Jul-20	4	A flaw was discovered in	https://bugz	A-RED-AMQ-

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Resource Consumption			Wildfly's EJB Client as shipped with Red Hat JBoss EAP 7, where some specific EJB transaction objects may get accumulated over the time and can cause services to slow down and eventaully unavailable. An attacker can take advantage and cause denial of service attack and make services unavailable. **CVE ID : CVE-2020-14297**	illa.redhat.com/show_bug.cgi?id=CVE-2020-14297	190820/508
openshift_virtualization					
Improper Privilege Management	29-Jul-20	6.5	A flaw was found in kubevirt 0.29 and earlier. Virtual Machine Instances (VMIs) can be used to gain access to the host's filesystem. Successful exploitation allows an attacker to assume the privileges of the VM process on the host system. In worst-case scenarios an attacker can read and modify any file on the system where the VMI is running. The highest threat from this vulnerability is to data confidentiality and integrity as well as system availability. **CVE ID : CVE-2020-14316**	N/A	A-RED-OPEN-190820/509
openshift_container_platform					
Improper Verification	29-Jul-20	4.4	GRUB2 fails to validate kernel signature when	https://lists.gnu.org/arch	A-RED-OPEN-190820/510

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
of Cryptographic Signature			booted directly without shim, allowing secure boot to be bypassed. This only affects systems where the kernel signing certificate has been imported directly into the secure boot database and the GRUB image is booted directly without the use of shim. This issue affects GRUB2 version 2.04 and prior versions. **CVE ID : CVE-2020-15705**	ive/html/grub-devel/2020-07/msg00034.html, https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/ADV200011, https://security.netapp.com/advisory/ntap-20200731-0008/	
Concurrent Execution using Shared Resource with Improper Synchronization ('Race Condition')	29-Jul-20	4.4	GRUB2 contains a race condition in grub_script_function_create() leading to a use-after-free vulnerability which can be triggered by redefining a function whilst the same function is already executing, leading to arbitrary code execution and secure boot restriction bypass. This issue affects GRUB2 version 2.04 and prior versions. **CVE ID : CVE-2020-15706**	https://lists.gnu.org/archive/html/grub-devel/2020-07/msg00034.html, https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/ADV200011, https://security.netapp.com/advisory/ntap-20200731-0008/	A-RED-OPEN-190820/511
Concurrent Execution using Shared	29-Jul-20	4.4	Integer overflows were discovered in the functions grub_cmd_initrd and	https://lists.gnu.org/archive/html/gru	A-RED-OPEN-190820/512

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Resource with Improper Synchronization ('Race Condition')			grub_initrd_init in the efilinux component of GRUB2, as shipped in Debian, Red Hat, and Ubuntu (the functionality is not included in GRUB2 upstream), leading to a heap-based buffer overflow. These could be triggered by an extremely large number of arguments to the initrd command on 32-bit architectures, or a crafted filesystem with very large files on any architecture. An attacker could use this to execute arbitrary code and bypass UEFI Secure Boot restrictions. This issue affects GRUB2 version 2.04 and prior versions. **CVE ID : CVE-2020-15707**	b-devel/2020-07/msg00034.html, https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/ADV200011, https://security.netapp.com/advisory/ntap-20200731-0008/	
satellite					
Insufficiently Protected Credentials	31-Jul-20	4.6	A flaw was found in Red Hat Satellite 6 which allows privileged attacker to read cache files. These cache credentials could help attacker to gain complete control of the Satellite instance. **CVE ID : CVE-2020-14334**	N/A	A-RED-SATE-190820/513
ansible_tower					
Information Exposure Through an Error	31-Jul-20	5	A data exposure flaw was found in Tower, where sensitive data was revealed from the HTTP	N/A	A-RED-ANSI-190820/514

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Message			return error codes. This flaw allows an unauthenticated, remote attacker to retrieve pages from the default organization and verify existing usernames. The highest threat from this vulnerability is to data confidentiality. **CVE ID : CVE-2020-14337**		
ripe					
rpki_validator_3					
Improper Certificate Validation	30-Jul-20	5	** DISPUTED ** An issue was discovered in RIPE NCC RPKI Validator 3.x through 3.1-2020.07.06.14.28. Missing validation checks on CRL presence or CRL staleness in the X509-based RPKI certificate-tree validation procedure allow remote attackers to bypass intended access restrictions by using revoked certificates. NOTE: there may be counterarguments related to backwards compatibility. **CVE ID : CVE-2020-16162**	N/A	A-RIP-RPKI-190820/515
Improper Certificate Validation	30-Jul-20	6.4	** DISPUTED ** An issue was discovered in RIPE NCC RPKI Validator 3.x before 3.1-2020.07.06.14.28. RRDP fetches proceed even with a lack of validation of a	N/A	A-RIP-RPKI-190820/516

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			TLS HTTPS endpoint. This allows remote attackers to bypass intended access restrictions, or to trigger denial of service to traffic directed to co-dependent routing systems. NOTE: third parties assert that the behavior is intentionally permitted by RFC 8182. **CVE ID : CVE-2020-16163**		
Improper Certificate Validation	30-Jul-20	5.8	** DISPUTED ** An issue was discovered in RIPE NCC RPKI Validator 3.x through 3.1-2020.07.06.14.28. It allows remote attackers to bypass intended access restrictions or to cause a denial of service on dependent routing systems by strategically withholding RPKI Route Origin Authorisation ".roa" files or X509 Certificate Revocation List files from the RPKI relying party's view. NOTE: some third parties may regard this as a preferred behavior, not a vulnerability. **CVE ID : CVE-2020-16164**	N/A	A-RIP-RPKI-190820/517
Riverbed					
steelcentral_aternity_agent					
Improper Limitation of a Pathname to a	27-Jul-20	5	SteelCentral Aternity Agent before 11.0.0.120 on Windows allows Privilege Escalation via a crafted	https://aternity.force.com/customersuccess/s/artic	A-RIV-STEE-190820/518

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Restricted Directory ('Path Traversal')			file. It uses an executable running as a high privileged Windows service to perform administrative tasks and collect data from other processes. It distributes functionality among different processes and uses IPC (Inter-Process Communication) primitives to enable the processes to cooperate. The remotely callable methods from remotable objects available through interprocess communication allow loading of arbitrary plugins (i.e., C# assemblies) from the "%PROGRAMFILES(X86) %/Aternity Information Systems/Assistant/plugins ” directory, where the name of the plugin is passed as part of an XML-serialized object. However, because the name of the DLL is concatenated with the “.\plugins” string, a directory traversal vulnerability exists in the way plugins are resolved. **CVE ID : CVE-2020-15592**	le/Recorder-tool-security-notification-mitigation-steps-for-On-Prem	
Incorrect Permission Assignment for Critical Resource	27-Jul-20	7.2	SteelCentral Aternity Agent 11.0.0.120 on Windows mishandles IPC. It uses an executable running as a high privileged Windows	https://aternity.force.com/customersuccess/s/article/Recorder-tool-	A-RIV-STEE-190820/519

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			service to perform administrative tasks and collect data from other processes. It distributes functionality among different processes and uses IPC (Inter-Process Communication) primitives to enable the processes to cooperate. Any user in the system is allowed to access the interprocess communication channel AternityAgentAssistantIpc, retrieve a serialized object and call object methods remotely. Among others, the methods allow any user to: (1) Create and/or overwrite arbitrary XML files across the system; (2) Create arbitrary directories across the system; and (3) Load arbitrary plugins (i.e., C# assemblies) from the "%PROGRAMFILES(X86)/ Aternity Information Systems/Assistant/plugins " directory and execute code contained in them. **CVE ID : CVE-2020-15593**	security-notification-mitigation-steps-for-On-Prem	
Rockwellautomation					
factorytalk_view					
Information Exposure	20-Jul-20	4	All versions of FactoryTalk View SE disclose the hostnames and file paths for certain files within the system. A remote,	N/A	A-ROC-FACT-190820/520

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			authenticated attacker may be able to leverage this information for reconnaissance efforts. Rockwell Automation recommends enabling built in security features found within FactoryTalk View SE. Users should follow guidance found in knowledge base articles 109056 and 1126943 to set up IPSec and/or HTTPs. **CVE ID : CVE-2020-12027**		
Improper Preservation of Permissions	20-Jul-20	5.5	In all versions of FactoryTalk View SEA remote, an authenticated attacker may be able to utilize certain handlers to interact with the data on the remote endpoint since those handlers do not enforce appropriate permissions. Rockwell Automation recommends enabling built in security features found within FactoryTalk View SE. Users should follow guidance found in knowledge base articles 109056 and 1126943 to set up IPSec and/or HTTPs. **CVE ID : CVE-2020-12028**	N/A	A-ROC-FACT-190820/521
Improper Input Validation	20-Jul-20	6.8	All versions of FactoryTalk View SE do not properly validate input of filenames within a project directory.	N/A	A-ROC-FACT-190820/522

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			A remote, unauthenticated attacker may be able to execute a crafted file on a remote endpoint that may result in remote code execution (RCE). Rockwell Automation recommends applying patch 1126289. Before installing this patch, the patch rollup dated 06 Apr 2020 or later MUST be applied. 1066644 – Patch Roll-up for CPR9 SRx. **CVE ID : CVE-2020-12029**		
Improper Restriction of Operations within the Bounds of a Memory Buffer	20-Jul-20	4.6	In all versions of FactoryTalk View SE, after bypassing memory corruption mechanisms found in the operating system, a local, authenticated attacker may corrupt the associated memory space allowing for arbitrary code execution. Rockwell Automation recommends applying patch 1126290. Before installing this patch, the patch rollup dated 06 Apr 2020 or later MUST be applied. 1066644 – Patch Roll-up for CPR9 SRx. **CVE ID : CVE-2020-12031**	N/A	A-ROC-FACT-190820/523
rollup-plugin-dev-server_project					
rollup-plugin-dev-server					
Improper Limitation of a Pathname	25-Jul-20	5	This affects all versions of package rollup-plugin-dev-server. There is no path	N/A	A-ROL-ROLL-190820/524

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
to a Restricted Directory ('Path Traversal')			sanitization in readFile operation inside the readFileFromContentBase function. **CVE ID : CVE-2020-7686**		
rollup-plugin-serve_project					
rollup-plugin-serve					
Improper Limitation of a Pathname to a Restricted Directory ('Path Traversal')	17-Jul-20	7.5	This affects all versions of package rollup-plugin-serve. There is no path sanitization in readFile operation. **CVE ID : CVE-2020-7684**	N/A	A-ROL-ROLL-190820/525
rollup-plugin-server_project					
rollup-plugin-server					
Improper Limitation of a Pathname to a Restricted Directory ('Path Traversal')	25-Jul-20	5	This affects all versions of package rollup-plugin-server. There is no path sanitization in readFile operation performed inside the readFileFromContentBase function. **CVE ID : CVE-2020-7683**	N/A	A-ROL-ROLL-190820/526
RSA					
multifactor_authentication_agent					
Improper Authenticati on	31-Jul-20	7.2	Authentication Bypass Vulnerability RSA MFA Agent 2.0 for Microsoft Windows contains an Authentication Bypass vulnerability. A local unauthenticated attacker could potentially exploit this vulnerability by using an alternate path to bypass	N/A	A-RSA-MULT-190820/527

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			authentication in order to gain full access to the system. **CVE ID : CVE-2020-5384**		
Schneider-electric					
easergy_builder					
Use of a Broken or Risky Cryptographic Algorithm	23-Jul-20	4.6	A CWE-327: Use of a Broken or Risky Cryptographic Algorithm vulnerability exists in Easergy Builder (Version 1.4.7.2 and older) which could allow an attacker access to the authorization credentials for a device and gain full access. **CVE ID : CVE-2020-7514**	N/A	A-SCH-EASE-190820/528
Use of Hard-coded Credentials	23-Jul-20	2.1	A CWE-321: Use of hard-coded cryptographic key stored in cleartext vulnerability exists in Easergy Builder (Version 1.4.7.2 and older) which could allow an attacker to decrypt a password. **CVE ID : CVE-2020-7515**	N/A	A-SCH-EASE-190820/529
Cleartext Storage of Sensitive Information	23-Jul-20	2.1	A CWE-316: Cleartext Storage of Sensitive Information in Memory vulnerability exists in Easergy Builder (Version 1.4.7.2 and older) which could allow an attacker access to login credentials. **CVE ID : CVE-2020-7516**	N/A	A-SCH-EASE-190820/530
Cleartext Storage of Sensitive	23-Jul-20	2.1	A CWE-312: Cleartext Storage of Sensitive Information vulnerability	N/A	A-SCH-EASE-190820/531

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Information			exists in Easergy Builder (Version 1.4.7.2 and older) which could allow an attacker to read user credentials. **CVE ID : CVE-2020-7517**		
Improper Input Validation	23-Jul-20	5	A CWE-20: Improper input validation vulnerability exists in Easergy Builder (Version 1.4.7.2 and older) which could allow an attacker to modify project configuration files. **CVE ID : CVE-2020-7518**	N/A	A-SCH-EASE-190820/532
Weak Password Requirements	23-Jul-20	5	A CWE-521: Weak Password Requirements vulnerability exists in Easergy Builder (Version 1.4.7.2 and older) which could allow an attacker to compromise a user account. **CVE ID : CVE-2020-7519**	N/A	A-SCH-EASE-190820/533
software_update_utility					
URL Redirection to Untrusted Site ('Open Redirect')	23-Jul-20	4	A CWE-601: URL Redirection to Untrusted Site ('Open Redirect') vulnerability exists in Schneider Electric Software Update (SESU), V2.4.0 and prior, which could cause execution of malicious code on the victim's machine. In order to exploit this vulnerability, an attacker requires privileged access on the engineering workstation to modify a	N/A	A-SCH-SOFT-190820/534

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Windows registry key which would divert all traffic updates to go through a server in the attacker's possession. A man-in-the-middle attack is then used to complete the exploit. **CVE ID : CVE-2020-7520**		
seafile					
seafile-client					
Uncontrolled Search Path Element	29-Jul-20	4.4	The seafile-client client 7.0.8 for Seafile is vulnerable to DLL hijacking because it loads exchndl.dll from the current working directory. **CVE ID : CVE-2020-16143**	N/A	A-SEA-SEAF-190820/535
servey_project					
servey					
Improper Limitation of a Pathname to a Restricted Directory ('Path Traversal')	20-Jul-20	5	A path traversal vulnerability in servey version < 3 allows an attacker to read content of any arbitrary file. **CVE ID : CVE-2020-8214**	N/A	A-SER-SERV-190820/536
Shopware					
shopware					
Server-Side Request Forgery (SSRF)	28-Jul-20	6.5	Shopware before 6.2.3 is vulnerable to a Server-Side Request Forgery (SSRF) in its "Mediabrowser upload by URL" feature. This allows an authenticated user to send HTTP, HTTPS, FTP, and SFTP requests on	https://docs.shopware.com/en/shopware-6-en/security-updates/security-update-07-2020,	A-SHO-SHOP-190820/537

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			behalf of the Shopware platform server. **CVE ID : CVE-2020-13970**	https://www.shopware.com/en/changelog/#6-2-3	
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	28-Jul-20	3.5	In Shopware before 6.2.3, authenticated users are allowed to use the Mediabrowser fileupload feature to upload SVG images containing JavaScript. This leads to Persistent XSS. An uploaded image can be accessed without authentication. **CVE ID : CVE-2020-13971**	https://docs.shopware.com/en/shopware-6-en/security-updates/security-update-07-2020, https://www.shopware.com/en/changelog/#6-2-3	A-SHO-SHOP-190820/538
Insufficiently Protected Credentials	28-Jul-20	5	In Shopware before 6.2.3, the database password is leaked to an unauthenticated user when a DriverException occurs and verbose error handling is enabled. **CVE ID : CVE-2020-13997**	https://docs.shopware.com/en/shopware-6-en/security-updates/security-update-07-2020, https://www.shopware.com/en/changelog/#6-2-3	A-SHO-SHOP-190820/539
sick					
package_analytics					
Improper Authentication	29-Jul-20	7.5	SICK Package Analytics software up to and including version V04.0.0 are vulnerable to an authentication bypass by directly interfacing with the REST API. An attacker	N/A	A-SIC-PACK-190820/540

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			can send unauthorized requests, bypass current authentication controls presented by the application and could potentially write files without authentication. **CVE ID : CVE-2020-2076**		
Incorrect Default Permissions	29-Jul-20	5	SICK Package Analytics software up to and including version V04.0.0 are vulnerable due to incorrect default permissions settings. An unauthorized attacker could read sensitive data from the system by querying for known files using the REST API directly. **CVE ID : CVE-2020-2077**	N/A	A-SIC-PACK-190820/541
Insufficiently Protected Credentials	29-Jul-20	4	Passwords are stored in plain text within the configuration of SICK Package Analytics software up to and including V04.1.1. An authorized attacker could access these stored plaintext credentials and gain access to the ftp service. Storing a password in plaintext allows attackers to easily gain access to systems, potentially compromising personal information or other sensitive information.	N/A	A-SIC-PACK-190820/542

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2020-2078		
simpleledger					
slp-validate					
Incorrect Comparison	30-Jul-20	5	In SLP Validate (npm package slp-validate) before version 1.2.2, there is a vulnerability to false-positive validation outcomes for the NFT1 Child Genesis transaction type. A poorly implemented SLP wallet or opportunistic attacker could create a seemingly valid NFT1 child token without burning any of the NFT1 Group token type as is required by the NFT1 specification. This is fixed in version 1.2.2. **CVE ID : CVE-2020-15131**	https://github.com/simpleledger/slp-validate.js/security/advisories/GHSA-6jmr-jfh7-xg3h	A-SIM-SLP--190820/543
slpjs					
Incorrect Comparison	30-Jul-20	5	In SLPJS (npm package slpjs) before version 0.27.4, there is a vulnerability to false-positive validation outcomes for the NFT1 Child Genesis transaction type. A poorly implemented SLP wallet or opportunistic attacker could create a seemingly valid NFT1 child token without burning any of the NFT1 Group token type as is required by the NFT1 specification. This is fixed in version 0.27.4.	https://github.com/simpleledger/slpjs/security/advisories/GHSA-cc2p-4jhr-xhhx	A-SIM-SLPJ-190820/544

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2020-15130		
Sonatype					
nexus_repository_manager_3					
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	31-Jul-20	4.3	Sonatype Nexus Repository Manager OSS/Pro versions before 3.25.1 allow XSS (issue 1 of 2). **CVE ID : CVE-2020-15869**	https://support.sonatype.com/hc/en-us/articles/360051424554	A-SON-NEXU-190820/545
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	31-Jul-20	4.3	Sonatype Nexus Repository Manager OSS/Pro versions before 3.25.1 allow XSS (Issue 2 of 2). **CVE ID : CVE-2020-15870**	https://support.sonatype.com/hc/en-us/articles/360051424754	A-SON-NEXU-190820/546
Incorrect Permission Assignment for Critical Resource	31-Jul-20	6.8	Sonatype Nexus Repository Manager OSS/Pro version before 3.25.1 allows Remote Code Execution. **CVE ID : CVE-2020-15871**	https://support.sonatype.com/hc/en-us/articles/360052192693	A-SON-NEXU-190820/547
Sonicwall					
netextender					
Improper Input Validation	17-Jul-20	4.6	SonicWall NetExtender Windows client vulnerable to arbitrary file write vulnerability, this allows attacker to overwrite a DLL and execute code with the same privilege in the host operating system. This vulnerability impact SonicWall NetExtender Windows client version	https://psirt.global.sonicwall.com/vuln-detail/SNWLID-2020-0004	A-SON-NETE-190820/548

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			9.0.815 and earlier. **CVE ID : CVE-2020-5131**		
springblade_project					
springblade					
Improper Neutralization of Special Elements used in an SQL Command ('SQL Injection')	30-Jul-20	7.5	The DAO/DTO implementation in SpringBlade through 2.7.1 allows SQL Injection in an ORDER BY clause. This is related to the /api/blade-log/api/list ascs and desc parameters. **CVE ID : CVE-2020-16165**	N/A	A-SPR-SPRI-190820/549
tc_custom_javascript_project					
tc_custom_javascript					
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	21-Jul-20	4.3	A stored Cross-Site Scripting (XSS) vulnerability in the TC Custom JavaScript plugin before 1.2.2 for WordPress allows unauthenticated remote attackers to inject arbitrary JavaScript via the tccj-content parameter. This is displayed in the page footer of every front-end page and executed in the browser of visitors. **CVE ID : CVE-2020-14063**	N/A	A-TC_-TC_C-190820/550
Teamviewer					
teamviewer					
Unquoted Search Path or Element	29-Jul-20	6.8	TeamViewer Desktop for Windows before 15.8.3 does not properly quote its custom URI handlers. A malicious website could launch TeamViewer with	https://community.teamviewer.com/t5/Announcements/Statement-on-	A-TEA-TEAM-190820/551

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			arbitrary parameters, as demonstrated by a teamviewer10: --play URL. An attacker could force a victim to send an NTLM authentication request and either relay the request or capture the hash for offline password cracking. This affects teamviewer10, teamviewer8, teamviewerapi, tvchat1, tvcontrol1, tvfiletransfer1, tvjoinv8, tvpresent1, tvsendfile1, tvsqcustomer1, tvsqsupport1, tvvideocall1, and tvvpn1. The issue is fixed in 8.0.258861, 9.0.258860, 10.0.258873, 11.0.258870, 12.0.258869, 13.2.36220, 14.2.56676, 14.7.48350, and 15.8.3. **CVE ID : CVE-2020-13699**	CVE-2020-13699/td-p/98448	
tgstation13					
tgstation-server					
Incorrect Permission Assignment for Critical Resource	31-Jul-20	6.8	In tgstation-server 4.4.0 and 4.4.1, an authenticated user with permission to download logs can download any file on the server machine (accessible by the owner of the server process) via directory traversal ../ sequences in /Administration/Logs/ requests. The attacker is unable to enumerate files, however.	N/A	A-TGS-TGST-190820/552

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2020-16136		
tobesoft					
miplatform					
Improper Neutralization of Special Elements used in an OS Command ('OS Command Injection')	17-Jul-20	10	A vulnerability exists that could allow the execution of operating system commands on systems running MiPlatform 2019.05.16 and earlier. An attacker could execute arbitrary remote command by sending parameters to WinExec function in ExtCommandApi.dll module of MiPlatform. **CVE ID : CVE-2020-7825**	https://www.boho.or.kr/krcert/secNoticeView.do?bulletin_writing_sequence=35509	A-TOB-MIPL-190820/553
torchbox					
wagtail					
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	20-Jul-20	3.5	In Wagtail before versions 2.7.4 and 2.9.3, when a form page type is made available to Wagtail editors through the `wagtail.contrib.forms` app, and the page template is built using Django's standard form rendering helpers such as form.as_p, any HTML tags used within a form field's help text will be rendered unescaped in the page. Allowing HTML within help text is an intentional design decision by Django; however, as a matter of policy Wagtail does not allow editors to insert	https://github.com/wagtail/wagtail/security/advisories/GHSA-2473-9hgq-j7xw	A-TOR-WAGT-190820/554

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			arbitrary HTML by default, as this could potentially be used to carry out cross-site scripting attacks, including privilege escalation. This functionality should therefore not have been made available to editor-level users. The vulnerability is not exploitable by an ordinary site visitor without access to the Wagtail admin. Patched versions have been released as Wagtail 2.7.4 (for the LTS 2.7 branch) and Wagtail 2.9.3 (for the current 2.9 branch). In these versions, help text will be escaped to prevent the inclusion of HTML tags. Site owners who wish to re-enable the use of HTML within help text (and are willing to accept the risk of this being exploited by editors) may set WAGTAILFORMS_HELP_TEXT_ALLOW_HTML = True in their configuration settings. Site owners who are unable to upgrade to the new versions can secure their form page templates by rendering forms field-by-field as per Django's documentation, but omitting the |safe filter when outputting the help text.		

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2020-15118		
toyota					
global_techstream					
Improper Restriction of Operations within the Bounds of a Memory Buffer	30-Jul-20	9.3	Global TechStream (GTS) for TOYOTA dealers version 15.10.032 and earlier allows an attacker to cause a denial-of-service (DoS) condition and execute arbitrary code via unspecified vectors. **CVE ID : CVE-2020-5610**	N/A	A-TOY-GLOB-190820/555
transloadit					
uppy					
Server-Side Request Forgery (SSRF)	20-Jul-20	5	The uppy npm package < 1.13.2 and < 2.0.0-alpha.5 is vulnerable to a Server-Side Request Forgery (SSRF) vulnerability, which allows an attacker to scan local or external networks or otherwise interact with internal systems. **CVE ID : CVE-2020-8205**	N/A	A-TRA-UPPY-190820/556
trusteddomain					
opendmarc					
Out-of-bounds Write	27-Jul-20	7.5	OpenDMARC through 1.3.2 and 1.4.x through 1.4.0-Beta1 has improper null termination in the function opendmarc_xml_parse that can result in a one-byte heap overflow in opendmarc_xml when parsing a specially crafted DMARC aggregate report. This can cause remote	N/A	A-TRU-OPEN-190820/557

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			memory corruption when a '\0' byte overwrites the heap metadata of the next chunk and its PREV_INUSE flag. **CVE ID : CVE-2020-12460**		
Typo3					
typo3					
Deserialization of Untrusted Data	29-Jul-20	6.5	In TYPO3 CMS greater than or equal to 9.0.0 and less than 9.5.20, and greater than or equal to 10.0.0 and less than 10.4.6, it has been discovered that an internal verification mechanism can be used to generate arbitrary checksums. This allows to inject arbitrary data having a valid cryptographic message authentication code (HMAC-SHA1) and can lead to various attack chains including potential privilege escalation, insecure deserialization & remote code execution. The overall severity of this vulnerability is high based on mentioned attack chains and the requirement of having a valid backend user session (authenticated). This has been patched in versions 9.5.20 and 10.4.6. **CVE ID : CVE-2020-15098**	https://github.com/TYPO3/TYPO3.CMS/security/advisories/GHSA-m5vr-3m74-jwxp	A-TYP-TYPO-190820/558
Improper	29-Jul-20	6.8	In TYPO3 CMS greater	https://githu	A-TYP-TYPO-

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Input Validation			than or equal to 9.0.0 and less than 9.5.20, and greater than or equal to 10.0.0 and less than 10.4.6, in a case where an attacker manages to generate a valid cryptographic message authentication code (HMAC-SHA1) - either by using a different existing vulnerability or in case the internal encryptionKey was exposed - it is possible to retrieve arbitrary files of a TYPO3 installation. This includes the possibility to fetch typo3conf/LocalConfiguration.php, which again contains the encryptionKey as well as credentials of the database management system being used. In case a database server is directly accessible either via internet or in a shared hosting network, this allows the ability to completely retrieve, manipulate or delete database contents. This includes creating an administration user account - which can be used to trigger remote code execution by injecting custom extensions. This has been patched in versions 9.5.20 and 10.4.6.	b.com/TYPO3/TYPO3.CMS/security/advisories/GHSA-3x94-fv5h-5q2c	190820/559

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2020-15099		
mediace					
Deserialization of Untrusted Data	29-Jul-20	7.5	In TYPO3 installations with the "mediace" extension from version 7.6.2 and before version 7.6.5, it has been discovered that an internal verification mechanism can be used to generate arbitrary checksums. The allows to inject arbitrary data having a valid cryptographic message authentication code and can lead to remote code execution. To successfully exploit this vulnerability, an attacker must have access to at least one `Extbase` plugin or module action in a TYPO3 installation. This is fixed in version 7.6.5 of the "mediace" extension for TYPO3. **CVE ID : CVE-2020-15086**	https://github.com/FriendsOfTYPO3/mediace/security/advisories/GHSA-4h44-w6fm-548g	A-TYP-MEDI-190820/560
ui					
unifi_protect					
Information Exposure Through an Error Message	30-Jul-20	5	An information exposure vulnerability exists in UniFi Protect before v1.13.4-beta.5 that allowed unauthenticated attackers access to valid usernames for the UniFi Protect web application via HTTP response code and response timing.	N/A	A-UI-UNIF-190820/561

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2020-8213		
Umbraco					
umbracoforms					
N/A	28-Jul-20	5	This affects all versions of package UmbracoForms. When using the default configuration for upload forms, it is possible to upload arbitrary file types. The package offers a way for users to mitigate the issue. The users of this package can create a custom workflow and frontend validation that blocks certain file types, depending on their security needs and policies. **CVE ID : CVE-2020-7685**	https://snyk.io/vuln/SNYK-DOTNET-UMBRACOFORMS-595765	A-UMB-UMBR-190820/562
Vmware					
gemfire					
Missing Authorization	31-Jul-20	6.5	VMware GemFire versions prior to 9.10.0, 9.9.2, 9.8.7, and 9.7.6, and VMware Tanzu GemFire for VMs versions prior to 1.11.1 and 1.10.2, when deployed without a SecurityManager, contain a JMX service available which contains an insecure default configuration. This allows a malicious user to create an MLet mbean leading to remote code execution. **CVE ID : CVE-2020-5396**	https://tanzu.vmware.com/security/cve-2020-5396	A-VMW-GEMF-190820/563

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
tanzu_gemfire_for_virtual_machines					
Missing Authorization	31-Jul-20	6.5	VMware GemFire versions prior to 9.10.0, 9.9.2, 9.8.7, and 9.7.6, and VMware Tanzu GemFire for VMs versions prior to 1.11.1 and 1.10.2, when deployed without a SecurityManager, contain a JMX service available which contains an insecure default configuration. This allows a malicious user to create an MLet mbean leading to remote code execution. **CVE ID : CVE-2020-5396**	https://tanzu.vmware.com/security/cve-2020-5396	A-VMW-TANZ-190820/564
spring_integration					
Deserialization of Untrusted Data	31-Jul-20	7.5	Spring Integration framework provides Kryo Codec implementations as an alternative for Java (de)serialization. When Kryo is configured with default options, all unregistered classes are resolved on demand. This leads to the "deserialization gadgets" exploit when provided data contains malicious code for execution during deserialization. In order to protect against this type of attack, Kryo can be configured to require a set of trusted classes for (de)serialization. Spring Integration should be proactive against blocking	https://tanzu.vmware.com/security/cve-2020-5413	A-VMW-SPRI-190820/565

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			unknown "deserialization gadgets" when configuring Kryo in code. **CVE ID : CVE-2020-5413**		
tanzu_application_service_for_virtual_machines					
Information Exposure Through Log Files	31-Jul-20	6	VMware Tanzu Application Service for VMs (2.7.x versions prior to 2.7.19, 2.8.x versions prior to 2.8.13, and 2.9.x versions prior to 2.9.7) contains an App Autoscaler that logs the UAA admin password. This credential is redacted on VMware Tanzu Operations Manager; however, the unredacted logs are available to authenticated users of the BOSH Director. This credential would grant administrative privileges to a malicious user. The same versions of App Autoscaler also log the App Autoscaler Broker password. Prior to newer versions of Operations Manager, this credential was not redacted from logs. This credential allows a malicious user to create, delete, and modify App Autoscaler services instances. Operations Manager started redacting this credential from logs as of its versions 2.7.15, 2.8.6, and 2.9.1. Note that these logs are typically only	https://tanzu.vmware.com/security/cve-2020-5414	A-VMW-TANZ-190820/566

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			visible to foundation administrators and operators. **CVE ID : CVE-2020-5414**		
operations_manager					
Information Exposure Through Log Files	31-Jul-20	6	VMware Tanzu Application Service for VMs (2.7.x versions prior to 2.7.19, 2.8.x versions prior to 2.8.13, and 2.9.x versions prior to 2.9.7) contains an App Autoscaler that logs the UAA admin password. This credential is redacted on VMware Tanzu Operations Manager; however, the unredacted logs are available to authenticated users of the BOSH Director. This credential would grant administrative privileges to a malicious user. The same versions of App Autoscaler also log the App Autoscaler Broker password. Prior to newer versions of Operations Manager, this credential was not redacted from logs. This credential allows a malicious user to create, delete, and modify App Autoscaler services instances. Operations Manager started redacting this credential from logs as of its versions 2.7.15, 2.8.6, and 2.9.1. Note that these logs are typically only	https://tanzu.vmware.com/security/cve-2020-5414	A-VMW-OPER-190820/567

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			visible to foundation administrators and operators. **CVE ID : CVE-2020-5414**		
westerndigital					
wd_discovery					
Improper Neutralization of Special Elements in Output Used by a Downstream Component ('Injection')	17-Jul-20	6.5	In Western Digital WD Discovery before 4.0.251.0, a malicious application running with standard user permissions could potentially execute code in the application's process through library injection by using DYLD environment variables. **CVE ID : CVE-2020-15816**	N/A	A-WES-WD_D-190820/568
wpsocialrocket					
social_sharing					
Cross-Site Request Forgery (CSRF)	27-Jul-20	6.8	Cross-site request forgery (CSRF) vulnerability in Social Sharing Plugin versions prior to 1.2.10 allows remote attackers to hijack the authentication of administrators via unspecified vectors. **CVE ID : CVE-2020-5611**	N/A	A-WPS-SOCI-190820/569
Zabbix					
Zabbix					
Improper Neutralization of Input During Web Page Generation ('Cross-site	17-Jul-20	4.3	Zabbix before 3.0.32rc1, 4.x before 4.0.22rc1, 4.1.x through 4.4.x before 4.4.10rc1, and 5.x before 5.0.2rc1 allows stored XSS in the URL Widget. **CVE ID : CVE-2020-15803**	N/A	A-ZAB-ZABB-190820/570

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Scripting')					
Zohocorp					
manageengine_desktop_central					
Integer Overflow or Wraparound	29-Jul-20	7.5	An issue was discovered in the client side of Zoho ManageEngine Desktop Central before 10.0.533. An attacker-controlled server can trigger an integer overflow via a crafted header value. **CVE ID : CVE-2020-15588**	https://www.manageengine.com/products/desktop-central/integer-overflow-vulnerability.html	A-ZOH-MANA-190820/571
Operating System					
abus					
secvest_hybrid_fumo50110_firmware					
Improper Authentication	30-Jul-20	6.4	The ABUS Secvest FUMO50110 hybrid module does not have any security mechanism that ensures confidentiality or integrity of RF packets that are exchanged with an alarm panel. This makes it easier to conduct wAppLoxx authentication-bypass attacks. **CVE ID : CVE-2020-14158**	N/A	O-ABU-SECV-190820/572
Apple					
iphone_os					
Incorrect Authorization	22-Jul-20	4.3	Incorrect security UI in basic auth in Google Chrome on iOS prior to 84.0.4147.89 allowed a remote attacker to spoof the contents of the Omnibox (URL bar) via a crafted HTML page.	N/A	O-APP-IPHO-190820/573

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2020-6528		
automationdirect					
c-more_hmi_ea9_firmware					
Improper Authentication	23-Jul-20	5	This vulnerability allows remote attackers to bypass authentication on affected installations of C-MORE HMI EA9 Firmware version 6.52 touch screen panels. Authentication is not required to exploit this vulnerability. The specific flaw exists within the authentication mechanism. The issue is due to insufficient authentication on post-authentication requests. An attacker can leverage this vulnerability to escalate privileges to resources normally protected from unauthenticated users. Was ZDI-CAN-10182. **CVE ID : CVE-2020-10918**	N/A	O-AUT-C-MO-190820/574
Weak Cryptography for Passwords	23-Jul-20	4.3	This vulnerability allows remote attackers to disclose sensitive information on affected installations of C-MORE HMI EA9 Firmware version 6.52 touch screen panels. Authentication is not required to exploit this vulnerability. The specific flaw exists within the handling of passwords. When transmitting passwords, the process encrypts them in a	N/A	O-AUT-C-MO-190820/575

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			recoverable format using a hard-coded key. An attacker can leverage this vulnerability to disclose credentials, leading to further compromise. Was ZDI-CAN-10185. **CVE ID : CVE-2020-10919**		
Missing Authenticati on for Critical Function	23-Jul-20	7.5	This vulnerability allows remote attackers to execute arbitrary code on affected installations of C-MORE HMI EA9 Firmware version 6.52 touch screen panels. Authentication is not required to exploit this vulnerability. The specific flaw exists within the control service, which listens on TCP port 9999 by default. The issue results from the lack of authentication prior to allowing alterations to the system configuration. An attacker can leverage this vulnerability to execute code in the context of the device. Was ZDI-CAN-10493. **CVE ID : CVE-2020-10920**	N/A	O-AUT-C-MO-190820/576
Missing Authenticati on for Critical Function	23-Jul-20	7.5	This vulnerability allows remote attackers to issue commands on affected installations of C-MORE HMI EA9 Firmware version 6.52 touch screen panels. Authentication is not required to exploit this vulnerability. The specific	N/A	O-AUT-C-MO-190820/577

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			flaw exists within the EA-HTTP.exe process. The issue results from the lack of authentication prior to allowing alterations to the system configuration. An attacker can leverage this vulnerability to issue commands to the physical equipment controlled by the device. Was ZDI-CAN-10482. **CVE ID : CVE-2020-10921**		
Improper Input Validation	23-Jul-20	5	This vulnerability allows remote attackers to create a denial-of-service condition on affected installations of C-MORE HMI EA9 Firmware version 6.52 touch screen panels. Authentication is not required to exploit this vulnerability. The specific flaw exists within the EA-HTTP.exe process. The issue results from the lack of proper input validation prior to further processing user requests. An attacker can leverage this vulnerability to create a denial-of-service condition on the system. Was ZDI-CAN-10527. **CVE ID : CVE-2020-10922**	N/A	O-AUT-C-MO-190820/578
avertx					
hd838_firmware					
N/A	23-Jul-20	7.2	An issue was discovered in AvertX Auto focus Night	N/A	O-AVE-HD83-190820/579

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Vision HD Indoor/Outdoor IP Dome Camera HD838 and Night Vision HD Indoor/Outdoor Mini IP Bullet Camera HD438. An attacker with physical access to the UART interface could access additional diagnostic and configuration functionalities as well as the camera's bootloader. Successful exploitation could compromise confidentiality, integrity, and availability of the affected system. It could even render the device inoperable. **CVE ID : CVE-2020-11623**		
Weak Password Requirements	23-Jul-20	7.5	An issue was discovered in AvertX Auto focus Night Vision HD Indoor/Outdoor IP Dome Camera HD838 and Night Vision HD Indoor/Outdoor Mini IP Bullet Camera HD438. They do not require users to change the default password for the admin account. They only show a pop-up window suggesting a change but there's no enforcement. An administrator can click Cancel and proceed to use the device without changing the password. Additionally, they disclose the default username within the login.js script.	N/A	O-AVE-HD83-190820/580

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Since many attacks for IoT devices, including malware and exploits, are based on the usage of default credentials, it makes these cameras an easy target for malicious actors. **CVE ID : CVE-2020-11624**		
Information Exposure Through Discrepancy	23-Jul-20	5	An issue was discovered in AvertX Auto focus Night Vision HD Indoor/Outdoor IP Dome Camera HD838 and Night Vision HD Indoor/Outdoor Mini IP Bullet Camera HD438. Failed web UI login attempts elicit different responses depending on whether a user account exists. Because the responses indicate whether a submitted username is valid or not, they make it easier to identify legitimate usernames. If a login request is sent to ISAPI/Security/sessionLogin/capabilities using a username that exists, it will return the value of the salt given to that username, even if the password is incorrect. However, if a login request is sent using a username that is not present in the database, it will return an empty salt value. This allows attackers to enumerate legitimate	N/A	O-AVE-HD83-190820/581

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			usernames, facilitating brute-force attacks. NOTE: this is different from CVE-2020-7057. **CVE ID : CVE-2020-11625**		
hd438_firmware					
N/A	23-Jul-20	7.2	An issue was discovered in AvertX Auto focus Night Vision HD Indoor/Outdoor IP Dome Camera HD838 and Night Vision HD Indoor/Outdoor Mini IP Bullet Camera HD438. An attacker with physical access to the UART interface could access additional diagnostic and configuration functionalities as well as the camera's bootloader. Successful exploitation could compromise confidentiality, integrity, and availability of the affected system. It could even render the device inoperable. **CVE ID : CVE-2020-11623**	N/A	O-AVE-HD43-190820/582
Weak Password Requirements	23-Jul-20	7.5	An issue was discovered in AvertX Auto focus Night Vision HD Indoor/Outdoor IP Dome Camera HD838 and Night Vision HD Indoor/Outdoor Mini IP Bullet Camera HD438. They do not require users to change the default password for the admin account. They only show a pop-up window suggesting	N/A	O-AVE-HD43-190820/583

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			a change but there's no enforcement. An administrator can click Cancel and proceed to use the device without changing the password. Additionally, they disclose the default username within the login.js script. Since many attacks for IoT devices, including malware and exploits, are based on the usage of default credentials, it makes these cameras an easy target for malicious actors. **CVE ID : CVE-2020-11624**		
Information Exposure Through Discrepancy	23-Jul-20	5	An issue was discovered in AvertX Auto focus Night Vision HD Indoor/Outdoor IP Dome Camera HD838 and Night Vision HD Indoor/Outdoor Mini IP Bullet Camera HD438. Failed web UI login attempts elicit different responses depending on whether a user account exists. Because the responses indicate whether a submitted username is valid or not, they make it easier to identify legitimate usernames. If a login request is sent to ISAPI/Security/sessionLogin/capabilities using a username that exists, it will return the value of the salt given to that	N/A	O-AVE-HD43-190820/584

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			username, even if the password is incorrect. However, if a login request is sent using a username that is not present in the database, it will return an empty salt value. This allows attackers to enumerate legitimate usernames, facilitating brute-force attacks. NOTE: this is different from CVE-2020-7057. **CVE ID : CVE-2020-11625**		
Canonical					
ubuntu_linux					
Improper Privilege Management	29-Jul-20	4.6	cloud-init as managed by snapd on Ubuntu Core 16 and Ubuntu Core 18 devices was run without restrictions on every boot, which a physical attacker could exploit by crafting cloud-init user-data/meta-data via external media to perform arbitrary changes on the device to bypass intended security mechanisms such as full disk encryption. This issue did not affect traditional Ubuntu systems. Fixed in snapd version 2.45.2, revision 8539 and core version 2.45.2, revision 9659. **CVE ID : CVE-2020-11933**	https://launchpad.net/bugs/1879530, https://ubuntu.com/USN-4424-1	O-CAN-UBUN-190820/585
Exposure of Resource to	29-Jul-20	1.9	It was discovered that snapctl user-open allowed	https://launchpad.net/b	O-CAN-UBUN-190820/586

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Wrong Sphere			altering the $XDG_DATA_DIRS environment variable when calling the system xdg-open. OpenURL() in usersession/userd/launcher.go would alter $XDG_DATA_DIRS to append a path to a directory controlled by the calling snap. A malicious snap could exploit this to bypass intended access restrictions to control how the host system xdg-open script opens the URL and, for example, execute a script shipped with the snap without confinement. This issue did not affect Ubuntu Core systems. Fixed in snapd versions 2.45.1ubuntu0.2, 2.45.1+18.04.2 and 2.45.1+20.04.2. **CVE ID : CVE-2020-11934**	ugs/1880085, https://ubuntu.com/USN-4424-1	
Improper Neutralization of Special Elements in Output Used by a Downstream Component ('Injection')	17-Jul-20	4.3	evolution-data-server (eds) through 3.36.3 has a STARTTLS buffering issue that affects SMTP and POP3. When a server sends a "begin TLS" response, eds reads additional data and evaluates it in a TLS context, aka "response injection." **CVE ID : CVE-2020-14928**	https://bugzilla.suse.com/show_bug.cgi?id=1173910, https://gitlab.gnome.org/GNOME//evolution-data-server/commit/ba82be72cfd427b5d72ff21f929b3a6d8529c4df	O-CAN-UBUN-190820/587

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
				, https://lists.debian.org/debian-lts-announce/2020/07/msg00012.html	
Improper Verification of Cryptographic Signature	29-Jul-20	4.4	GRUB2 fails to validate kernel signature when booted directly without shim, allowing secure boot to be bypassed. This only affects systems where the kernel signing certificate has been imported directly into the secure boot database and the GRUB image is booted directly without the use of shim. This issue affects GRUB2 version 2.04 and prior versions. **CVE ID : CVE-2020-15705**	https://lists.gnu.org/archive/html/grub-devel/2020-07/msg00034.html, https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/ADV200011, https://security.netapp.com/advisory/ntap-20200731-0008/	O-CAN-UBUN-190820/588
Concurrent Execution using Shared Resource with Improper Synchronization ('Race Condition')	29-Jul-20	4.4	GRUB2 contains a race condition in grub_script_function_create() leading to a use-after-free vulnerability which can be triggered by redefining a function whilst the same function is already executing, leading to arbitrary code execution and secure boot restriction bypass. This issue affects GRUB2 version 2.04 and	https://lists.gnu.org/archive/html/grub-devel/2020-07/msg00034.html, https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/ADV200011,	O-CAN-UBUN-190820/589

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			prior versions. **CVE ID : CVE-2020-15706**	https://security.netapp.com/advisory/ntap-20200731-0008/	
Concurrent Execution using Shared Resource with Improper Synchronization ('Race Condition')	29-Jul-20	4.4	Integer overflows were discovered in the functions grub_cmd_initrd and grub_initrd_init in the efilinux component of GRUB2, as shipped in Debian, Red Hat, and Ubuntu (the functionality is not included in GRUB2 upstream), leading to a heap-based buffer overflow. These could be triggered by an extremely large number of arguments to the initrd command on 32-bit architectures, or a crafted filesystem with very large files on any architecture. An attacker could use this to execute arbitrary code and bypass UEFI Secure Boot restrictions. This issue affects GRUB2 version 2.04 and prior versions. **CVE ID : CVE-2020-15707**	https://lists.gnu.org/archive/html/grub-devel/2020-07/msg00034.html, https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/ADV200011, https://security.netapp.com/advisory/ntap-20200731-0008/	O-CAN-UBUN-190820/590
Cisco					
rv130_firmware					
Improper Authentication	16-Jul-20	7.5	A vulnerability in the web-based management interface of the Cisco RV110W Wireless-N VPN Firewall, RV130 VPN	N/A	O-CIS-RV13-190820/591

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Router, RV130W Wireless-N Multifunction VPN Router, and RV215W Wireless-N VPN Router could allow an unauthenticated, remote attacker to bypass authentication and execute arbitrary commands with administrative commands on an affected device. The vulnerability is due to improper session management on affected devices. An attacker could exploit this vulnerability by sending a crafted HTTP request to the affected device. A successful exploit could allow the attacker to gain administrative access on the affected device. **CVE ID : CVE-2020-3144**		
Improper Restriction of Operations within the Bounds of a Memory Buffer	16-Jul-20	6.5	Multiple vulnerabilities in the web-based management interface of the Cisco RV110W Wireless-N VPN Firewall, RV130 VPN Router, RV130W Wireless-N Multifunction VPN Router, and RV215W Wireless-N VPN Router could allow an authenticated, remote attacker to execute arbitrary code on an affected device. The vulnerabilities are due to improper validation of user-supplied data in the web-based management	N/A	O-CIS-RV13-190820/592

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			interface. An attacker could exploit these vulnerabilities by sending malicious HTTP requests to a targeted device. A successful exploit could allow the attacker to execute arbitrary code on the underlying operating system of the affected device as a high-privilege user. **CVE ID : CVE-2020-3145**		
Improper Restriction of Operations within the Bounds of a Memory Buffer	16-Jul-20	9	Multiple vulnerabilities in the web-based management interface of the Cisco RV110W Wireless-N VPN Firewall, RV130 VPN Router, RV130W Wireless-N Multifunction VPN Router, and RV215W Wireless-N VPN Router could allow an authenticated, remote attacker to execute arbitrary code on an affected device. The vulnerabilities are due to improper validation of user-supplied data in the web-based management interface. An attacker could exploit these vulnerabilities by sending malicious HTTP requests to a targeted device. A successful exploit could allow the attacker to execute arbitrary code on the underlying operating system of the affected	N/A	O-CIS-RV13-190820/593

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			device as a high-privilege user. **CVE ID : CVE-2020-3146**		
sd-wan_firmware					
Improper Neutralization of Special Elements used in an SQL Command ('SQL Injection')	16-Jul-20	5.5	A vulnerability in the web-based management interface of Cisco SD-WAN vManage Software could allow an authenticated, remote attacker to conduct SQL injection attacks on an affected system. The vulnerability exists because the web-based management interface improperly validates values within SQL queries. An attacker could exploit this vulnerability by authenticating to the application and sending malicious SQL queries to an affected system. A successful exploit could allow the attacker to modify values on or return values from the underlying database or the operating system. **CVE ID : CVE-2020-3468**	N/A	O-CIS-SD-W-190820/594
Uncontrolled Resource Consumption	16-Jul-20	7.8	A vulnerability in Cisco SD-WAN Solution Software could allow an unauthenticated, remote attacker to cause a denial of service (DoS) condition. The vulnerability is due to improper validation of fields in Cisco SD-WAN peering messages that are	N/A	O-CIS-SD-W-190820/595

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			encapsulated in UDP packets. An attacker could exploit this vulnerability by sending crafted UDP messages to the targeted system. A successful exploit could allow the attacker to cause services on the device to fail, resulting in a DoS condition that could impact the targeted device and other devices that depend on it. **CVE ID : CVE-2020-3351**		
N/A	16-Jul-20	7.8	A vulnerability in the deep packet inspection (DPI) engine of Cisco SD-WAN vEdge Routers could allow an unauthenticated, remote attacker to cause a denial of service (DoS) condition on an affected device. The vulnerability is due to improper processing of FTP traffic. An attacker could exploit this vulnerability by sending crafted FTP packets through an affected device. A successful exploit could allow the attacker to make the device reboot continuously, causing a DoS condition. **CVE ID : CVE-2020-3369**	N/A	O-CIS-SD-W-190820/596
Uncontrolled Resource Consumption	16-Jul-20	4	A vulnerability in the web-based management interface of Cisco SD-WAN	N/A	O-CIS-SD-W-190820/597

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			vManage Software could allow an authenticated, remote attacker to consume excessive system memory and cause a denial of service (DoS) condition on an affected system. The vulnerability is due to inefficient memory management. An attacker could exploit this vulnerability by sending a large number of crafted HTTP requests to the affected web-based management interface. A successful exploit could allow the attacker to exhaust system memory, which could cause the system to stop processing new connections and could result in a DoS condition. **CVE ID : CVE-2020-3372**		
Improper Neutralization of Special Elements used in an SQL Command ('SQL Injection')	16-Jul-20	4	A vulnerability in the web-based management interface for Cisco SD-WAN vManage Software could allow an authenticated, remote attacker to impact the integrity of an affected system by executing arbitrary SQL queries. The vulnerability is due to insufficient validation of user-supplied input. An attacker could exploit this vulnerability by sending crafted input that includes SQL statements to an	N/A	O-CIS-SD-W-190820/598

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			affected system. A successful exploit could allow the attacker to modify entries in some database tables, affecting the integrity of the data. **CVE ID : CVE-2020-3378**		
Improper Input Validation	16-Jul-20	7.2	A vulnerability in Cisco SD-WAN Solution Software could allow an authenticated, local attacker to elevate privileges to Administrator on the underlying operating system. The vulnerability is due to insufficient input validation. An attacker could exploit this vulnerability by sending a crafted request to an affected system. A successful exploit could allow the attacker to gain administrative privileges. **CVE ID : CVE-2020-3379**	N/A	O-CIS-SD-W-190820/599
Improper Limitation of a Pathname to a Restricted Directory ('Path Traversal')	16-Jul-20	6.5	A vulnerability in the web management interface of Cisco SD-WAN vManage Software could allow an authenticated, remote attacker to conduct directory traversal attacks and obtain read and write access to sensitive files on a targeted system. The vulnerability is due to a lack of proper validation of files that are uploaded to an affected device. An	N/A	O-CIS-SD-W-190820/600

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			attacker could exploit this vulnerability by uploading a crafted file to an affected system. An exploit could allow the attacker to view or modify arbitrary files on the targeted system. **CVE ID : CVE-2020-3381**		
N/A	16-Jul-20	6.1	A vulnerability in the deep packet inspection (DPI) engine of Cisco SD-WAN vEdge Routers could allow an unauthenticated, adjacent attacker to cause a denial of service (DoS) condition on an affected system. The vulnerability is due to insufficient handling of malformed packets. An attacker could exploit this vulnerability by sending crafted packets through an affected device. A successful exploit could allow the attacker to cause the device to reboot, resulting in a DoS condition. **CVE ID : CVE-2020-3385**	N/A	O-CIS-SD-W-190820/601
Improper Input Validation	16-Jul-20	9	A vulnerability in Cisco SD-WAN vManage Software could allow an authenticated, remote attacker to execute code with root privileges on an affected system. The vulnerability is due to insufficient input sanitization during user authentication processing.	N/A	O-CIS-SD-W-190820/602

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			An attacker could exploit this vulnerability by sending a crafted response to the Cisco SD-WAN vManage Software. A successful exploit could allow the attacker to access the software and execute commands they should not be authorized to execute. **CVE ID : CVE-2020-3387**		
Improper Authenticati on	16-Jul-20	7.2	A vulnerability in the CLI of Cisco SD-WAN vManage Software could allow an authenticated, local attacker to inject arbitrary commands that are executed with root privileges. The vulnerability is due to insufficient input validation. An attacker could exploit this vulnerability by authenticating to the device and submitting crafted input to the CLI. The attacker must be authenticated to access the CLI. A successful exploit could allow the attacker to execute commands with root privileges. **CVE ID : CVE-2020-3388**	N/A	O-CIS-SD-W-190820/603
Improper Limitation of a Pathname to a Restricted	16-Jul-20	4	A vulnerability in the web-based management interface of Cisco SD-WAN vManage Software could allow an authenticated,	N/A	O-CIS-SD-W-190820/604

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Directory ('Path Traversal')			remote attacker to conduct path traversal attacks and obtain read access to sensitive files on an affected system. The vulnerability is due to insufficient validation of HTTP requests. An attacker could exploit this vulnerability by sending a crafted HTTP request that contains directory traversal character sequences to the affected system. A successful exploit could allow the attacker to view arbitrary files on the affected system. **CVE ID : CVE-2020-3401**		
Improper Restriction of XML External Entity Reference ('XXE')	16-Jul-20	4.9	A vulnerability in the web UI of Cisco SD-WAN vManage Software could allow an authenticated, remote attacker to gain read and write access to information that is stored on an affected system. The vulnerability is due to improper handling of XML External Entity (XXE) entries when parsing certain XML files. An attacker could exploit this vulnerability by persuading a user to import a crafted XML file with malicious entries. A successful exploit could allow the attacker to read and write files within the	N/A	O-CIS-SD-W-190820/605

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			affected application. **CVE ID : CVE-2020-3405**		
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	16-Jul-20	3.5	A vulnerability in the web-based management interface of the Cisco SD-WAN vManage Software could allow an authenticated, remote attacker to conduct a cross-site scripting (XSS) attack against a user of the interface. The vulnerability exists because the web-based management interface does not properly validate user-supplied input. An attacker could exploit this vulnerability by persuading a user to click a crafted link. A successful exploit could allow the attacker to execute arbitrary script code in the context of the interface or access sensitive, browser-based information. **CVE ID : CVE-2020-3406**	N/A	O-CIS-SD-W-190820/606
Improper Link Resolution Before File Access ('Link Following')	16-Jul-20	4	A vulnerability in the web-based management interface of Cisco SD-WAN vManage Software could allow an authenticated, remote attacker to read arbitrary files on the underlying filesystem of the device. The vulnerability is due to insufficient file scope limiting. An attacker could	N/A	O-CIS-SD-W-190820/607

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			exploit this vulnerability by creating a specific file reference on the filesystem and then accessing it through the web-based management interface. A successful exploit could allow the attacker to read arbitrary files from the filesystem of the underlying operating system. **CVE ID : CVE-2020-3437**		
rv110w_wireless-n_vpn_firewall_firmware					
Improper Restriction of Operations within the Bounds of a Memory Buffer	16-Jul-20	9	Multiple vulnerabilities in the web-based management interface of the Cisco RV110W Wireless-N VPN Firewall, RV130 VPN Router, RV130W Wireless-N Multifunction VPN Router, and RV215W Wireless-N VPN Router could allow an authenticated, remote attacker to execute arbitrary code on an affected device. The vulnerabilities are due to improper validation of user-supplied data in the web-based management interface. An attacker could exploit these vulnerabilities by sending malicious HTTP requests to a targeted device. A successful exploit could allow the attacker to execute arbitrary code on	N/A	O-CIS-RV11-190820/608

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			the underlying operating system of the affected device as a high-privilege user. **CVE ID : CVE-2020-3146**		
Improper Restriction of Operations within the Bounds of a Memory Buffer	16-Jul-20	10	A vulnerability in the web-based management interface of Cisco Small Business RV110W, RV130, RV130W, and RV215W Routers could allow an unauthenticated, remote attacker to execute arbitrary code on an affected device. The vulnerability is due to improper validation of user-supplied input in the web-based management interface. An attacker could exploit this vulnerability by sending crafted HTTP requests to a targeted device. A successful exploit could allow the attacker to execute arbitrary code as the root user on the underlying operating system of the affected device. **CVE ID : CVE-2020-3323**	N/A	O-CIS-RV11-190820/609
Use of Hard-coded Credentials	16-Jul-20	10	A vulnerability in the Telnet service of Cisco Small Business RV110W Wireless-N VPN Firewall Routers could allow an unauthenticated, remote attacker to take full control of the device with a high-	N/A	O-CIS-RV11-190820/610

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			privileged account. The vulnerability exists because a system account has a default and static password. An attacker could exploit this vulnerability by using this default account to connect to the affected system. A successful exploit could allow the attacker to gain full control of an affected device. **CVE ID : CVE-2020-3330**		
Improper Restriction of Operations within the Bounds of a Memory Buffer	16-Jul-20	10	A vulnerability in the web-based management interface of Cisco RV110W Wireless-N VPN Firewall and Cisco RV215W Wireless-N VPN Router could allow an unauthenticated, remote attacker to execute arbitrary code on an affected device. The vulnerability is due to improper validation of user-supplied input data by the web-based management interface. An attacker could exploit this vulnerability by sending crafted requests to a targeted device. A successful exploit could allow the attacker to execute arbitrary code with the privileges of the root user. **CVE ID : CVE-2020-3331**	N/A	O-CIS-RV11-190820/611

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Improper Neutralization of Special Elements used in an OS Command ('OS Command Injection')	16-Jul-20	9	A vulnerability in the web-based management interface of Cisco Small Business RV110W, RV130, RV130W, and RV215W Series Routers could allow an authenticated, remote attacker to inject arbitrary shell commands that are executed by an affected device. The vulnerability is due to insufficient input validation of user-supplied data. An attacker could exploit this vulnerability by sending a crafted request to the web-based management interface of an affected device. A successful exploit could allow the attacker to execute arbitrary shell commands or scripts with root privileges on the affected device. **CVE ID : CVE-2020-3332**	N/A	O-CIS-RV11-190820/612
rv130_vpn_router_firmware					
Improper Restriction of Operations within the Bounds of a Memory Buffer	16-Jul-20	10	A vulnerability in the web-based management interface of Cisco Small Business RV110W, RV130, RV130W, and RV215W Routers could allow an unauthenticated, remote attacker to execute arbitrary code on an affected device. The vulnerability is due to improper validation of user-supplied input in the	N/A	O-CIS-RV13-190820/613

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			web-based management interface. An attacker could exploit this vulnerability by sending crafted HTTP requests to a targeted device. A successful exploit could allow the attacker to execute arbitrary code as the root user on the underlying operating system of the affected device. **CVE ID : CVE-2020-3323**		
Improper Neutralization of Special Elements used in an OS Command ('OS Command Injection')	16-Jul-20	9	A vulnerability in the web-based management interface of Cisco Small Business RV110W, RV130, RV130W, and RV215W Series Routers could allow an authenticated, remote attacker to inject arbitrary shell commands that are executed by an affected device. The vulnerability is due to insufficient input validation of user-supplied data. An attacker could exploit this vulnerability by sending a crafted request to the web-based management interface of an affected device. A successful exploit could allow the attacker to execute arbitrary shell commands or scripts with root privileges on the affected device. **CVE ID : CVE-2020-3332**	N/A	O-CIS-RV13-190820/614

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
rv130w_wireless-n_multifunction_vpn_router_firmware					
Improper Restriction of Operations within the Bounds of a Memory Buffer	16-Jul-20	10	A vulnerability in the web-based management interface of Cisco Small Business RV110W, RV130, RV130W, and RV215W Routers could allow an unauthenticated, remote attacker to execute arbitrary code on an affected device. The vulnerability is due to improper validation of user-supplied input in the web-based management interface. An attacker could exploit this vulnerability by sending crafted HTTP requests to a targeted device. A successful exploit could allow the attacker to execute arbitrary code as the root user on the underlying operating system of the affected device. **CVE ID : CVE-2020-3323**	N/A	O-CIS-RV13-190820/615
Improper Neutralization of Special Elements used in an OS Command ('OS Command Injection')	16-Jul-20	9	A vulnerability in the web-based management interface of Cisco Small Business RV110W, RV130, RV130W, and RV215W Series Routers could allow an authenticated, remote attacker to inject arbitrary shell commands that are executed by an affected device. The vulnerability is due to insufficient input	N/A	O-CIS-RV13-190820/616

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			validation of user-supplied data. An attacker could exploit this vulnerability by sending a crafted request to the web-based management interface of an affected device. A successful exploit could allow the attacker to execute arbitrary shell commands or scripts with root privileges on the affected device. **CVE ID : CVE-2020-3332**		
rv215w_wireless-n_vpn_router_firmware					
Improper Restriction of Operations within the Bounds of a Memory Buffer	16-Jul-20	10	A vulnerability in the web-based management interface of Cisco Small Business RV110W, RV130, RV130W, and RV215W Routers could allow an unauthenticated, remote attacker to execute arbitrary code on an affected device. The vulnerability is due to improper validation of user-supplied input in the web-based management interface. An attacker could exploit this vulnerability by sending crafted HTTP requests to a targeted device. A successful exploit could allow the attacker to execute arbitrary code as the root user on the underlying operating system of the affected	N/A	O-CIS-RV21-190820/617

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			device. **CVE ID : CVE-2020-3323**		
Improper Restriction of Operations within the Bounds of a Memory Buffer	16-Jul-20	10	A vulnerability in the web-based management interface of Cisco RV110W Wireless-N VPN Firewall and Cisco RV215W Wireless-N VPN Router could allow an unauthenticated, remote attacker to execute arbitrary code on an affected device. The vulnerability is due to improper validation of user-supplied input data by the web-based management interface. An attacker could exploit this vulnerability by sending crafted requests to a targeted device. A successful exploit could allow the attacker to execute arbitrary code with the privileges of the root user. **CVE ID : CVE-2020-3331**	N/A	O-CIS-RV21-190820/618
Improper Neutralization of Special Elements used in an OS Command ('OS Command Injection')	16-Jul-20	9	A vulnerability in the web-based management interface of Cisco Small Business RV110W, RV130, RV130W, and RV215W Series Routers could allow an authenticated, remote attacker to inject arbitrary shell commands that are executed by an affected device. The vulnerability is due to insufficient input	N/A	O-CIS-RV21-190820/619

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			validation of user-supplied data. An attacker could exploit this vulnerability by sending a crafted request to the web-based management interface of an affected device. A successful exploit could allow the attacker to execute arbitrary shell commands or scripts with root privileges on the affected device. **CVE ID : CVE-2020-3332**		
rv340_dual_wan_gigabit_vpn_router_firmware					
Improper Input Validation	16-Jul-20	10	A vulnerability in the Secure Sockets Layer (SSL) VPN feature of Cisco Small Business RV340, RV340W, RV345, and RV345P Dual WAN Gigabit VPN Routers could allow an unauthenticated, remote attacker to execute arbitrary code on an affected device or cause the device to reload, resulting in a denial of service (DoS) condition. The vulnerability exists because HTTP requests are not properly validated. An attacker could exploit this vulnerability by sending a crafted HTTP request over an SSL connection to an affected device. A successful exploit could allow the attacker to remotely execute arbitrary	N/A	O-CIS-RV34-190820/620

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			code on the device or cause the device to reload, resulting in a DoS condition. **CVE ID : CVE-2020-3357**		
Improper Input Validation	16-Jul-20	7.8	A vulnerability in the Secure Sockets Layer (SSL) VPN feature for Cisco Small Business RV VPN Routers could allow an unauthenticated, remote attacker to cause the device to unexpectedly restart, causing a denial of service (DoS) condition. The vulnerability is due to a lack of proper input validation of HTTP requests. An attacker could exploit this vulnerability by sending a crafted HTTP request over an SSL connection to the targeted device. A successful exploit could allow the attacker to cause a reload, resulting in a DoS condition. **CVE ID : CVE-2020-3358**	N/A	O-CIS-RV34-190820/621
rv340w_dual_wan_gigabit_wireless-ac_vpn_router_firmware					
Improper Input Validation	16-Jul-20	10	A vulnerability in the Secure Sockets Layer (SSL) VPN feature of Cisco Small Business RV340, RV340W, RV345, and RV345P Dual WAN Gigabit VPN Routers could allow an unauthenticated, remote attacker to execute arbitrary code on an	N/A	O-CIS-RV34-190820/622

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			affected device or cause the device to reload, resulting in a denial of service (DoS) condition. The vulnerability exists because HTTP requests are not properly validated. An attacker could exploit this vulnerability by sending a crafted HTTP request over an SSL connection to an affected device. A successful exploit could allow the attacker to remotely execute arbitrary code on the device or cause the device to reload, resulting in a DoS condition. **CVE ID : CVE-2020-3357**		
Improper Input Validation	16-Jul-20	7.8	A vulnerability in the Secure Sockets Layer (SSL) VPN feature for Cisco Small Business RV VPN Routers could allow an unauthenticated, remote attacker to cause the device to unexpectedly restart, causing a denial of service (DoS) condition. The vulnerability is due to a lack of proper input validation of HTTP requests. An attacker could exploit this vulnerability by sending a crafted HTTP request over an SSL connection to the targeted device. A successful exploit could allow the attacker to cause	N/A	O-CIS-RV34-190820/623

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			a reload, resulting in a DoS condition. **CVE ID : CVE-2020-3358**		
rv345_dual_wan_gigabit_vpn_router_firmware					
Improper Input Validation	16-Jul-20	10	A vulnerability in the Secure Sockets Layer (SSL) VPN feature of Cisco Small Business RV340, RV340W, RV345, and RV345P Dual WAN Gigabit VPN Routers could allow an unauthenticated, remote attacker to execute arbitrary code on an affected device or cause the device to reload, resulting in a denial of service (DoS) condition. The vulnerability exists because HTTP requests are not properly validated. An attacker could exploit this vulnerability by sending a crafted HTTP request over an SSL connection to an affected device. A successful exploit could allow the attacker to remotely execute arbitrary code on the device or cause the device to reload, resulting in a DoS condition. **CVE ID : CVE-2020-3357**	N/A	O-CIS-RV34-190820/624
Improper Input Validation	16-Jul-20	7.8	A vulnerability in the Secure Sockets Layer (SSL) VPN feature for Cisco Small Business RV VPN Routers could allow an unauthenticated, remote	N/A	O-CIS-RV34-190820/625

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			attacker to cause the device to unexpectedly restart, causing a denial of service (DoS) condition. The vulnerability is due to a lack of proper input validation of HTTP requests. An attacker could exploit this vulnerability by sending a crafted HTTP request over an SSL connection to the targeted device. A successful exploit could allow the attacker to cause a reload, resulting in a DoS condition. **CVE ID : CVE-2020-3358**		
rv345p_dual_wan_gigabit_poe_vpn_router_firmware					
Improper Input Validation	16-Jul-20	10	A vulnerability in the Secure Sockets Layer (SSL) VPN feature of Cisco Small Business RV340, RV340W, RV345, and RV345P Dual WAN Gigabit VPN Routers could allow an unauthenticated, remote attacker to execute arbitrary code on an affected device or cause the device to reload, resulting in a denial of service (DoS) condition. The vulnerability exists because HTTP requests are not properly validated. An attacker could exploit this vulnerability by sending a crafted HTTP request over an SSL	N/A	O-CIS-RV34-190820/626

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			connection to an affected device. A successful exploit could allow the attacker to remotely execute arbitrary code on the device or cause the device to reload, resulting in a DoS condition. **CVE ID : CVE-2020-3357**		
Improper Input Validation	16-Jul-20	7.8	A vulnerability in the Secure Sockets Layer (SSL) VPN feature for Cisco Small Business RV VPN Routers could allow an unauthenticated, remote attacker to cause the device to unexpectedly restart, causing a denial of service (DoS) condition. The vulnerability is due to a lack of proper input validation of HTTP requests. An attacker could exploit this vulnerability by sending a crafted HTTP request over an SSL connection to the targeted device. A successful exploit could allow the attacker to cause a reload, resulting in a DoS condition. **CVE ID : CVE-2020-3358**	N/A	O-CIS-RV34-190820/627
rv110w_firmware					
Incorrect Authorizatio n	16-Jul-20	4.3	A vulnerability in the web-based management interface of Cisco Small Business RV110W and RV215W Series Routers could allow an	N/A	O-CIS-RV11-190820/628

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			unauthenticated, remote attacker to download sensitive information from the device, which could include the device configuration. The vulnerability is due to improper authorization of an HTTP request. An attacker could exploit this vulnerability by accessing a specific URI on the web-based management interface of the router, but only after any valid user has opened a specific file on the device since the last reboot. A successful exploit would allow the attacker to view sensitive information, which should be restricted. **CVE ID : CVE-2020-3150**		
Improper Authentication	16-Jul-20	7.5	A vulnerability in the web-based management interface of the Cisco RV110W Wireless-N VPN Firewall, RV130 VPN Router, RV130W Wireless-N Multifunction VPN Router, and RV215W Wireless-N VPN Router could allow an unauthenticated, remote attacker to bypass authentication and execute arbitrary commands with administrative commands on an affected device. The vulnerability is due to improper session	N/A	O-CIS-RV11-190820/629

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			management on affected devices. An attacker could exploit this vulnerability by sending a crafted HTTP request to the affected device. A successful exploit could allow the attacker to gain administrative access on the affected device. **CVE ID : CVE-2020-3144**		
Improper Restriction of Operations within the Bounds of a Memory Buffer	16-Jul-20	6.5	Multiple vulnerabilities in the web-based management interface of the Cisco RV110W Wireless-N VPN Firewall, RV130 VPN Router, RV130W Wireless-N Multifunction VPN Router, and RV215W Wireless-N VPN Router could allow an authenticated, remote attacker to execute arbitrary code on an affected device. The vulnerabilities are due to improper validation of user-supplied data in the web-based management interface. An attacker could exploit these vulnerabilities by sending malicious HTTP requests to a targeted device. A successful exploit could allow the attacker to execute arbitrary code on the underlying operating system of the affected device as a high-privilege user.	N/A	O-CIS-RV11-190820/630

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2020-3145		
rv130w_firmware					
Improper Authenticati on	16-Jul-20	7.5	A vulnerability in the web-based management interface of the Cisco RV110W Wireless-N VPN Firewall, RV130 VPN Router, RV130W Wireless-N Multifunction VPN Router, and RV215W Wireless-N VPN Router could allow an unauthenticated, remote attacker to bypass authentication and execute arbitrary commands with administrative commands on an affected device. The vulnerability is due to improper session management on affected devices. An attacker could exploit this vulnerability by sending a crafted HTTP request to the affected device. A successful exploit could allow the attacker to gain administrative access on the affected device. **CVE ID : CVE-2020-3144**	N/A	O-CIS-RV13-190820/631
Improper Restriction of Operations within the Bounds of a Memory Buffer	16-Jul-20	6.5	Multiple vulnerabilities in the web-based management interface of the Cisco RV110W Wireless-N VPN Firewall, RV130 VPN Router, RV130W Wireless-N Multifunction VPN Router, and RV215W Wireless-N VPN Router could allow an	N/A	O-CIS-RV13-190820/632

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			authenticated, remote attacker to execute arbitrary code on an affected device. The vulnerabilities are due to improper validation of user-supplied data in the web-based management interface. An attacker could exploit these vulnerabilities by sending malicious HTTP requests to a targeted device. A successful exploit could allow the attacker to execute arbitrary code on the underlying operating system of the affected device as a high-privilege user. **CVE ID : CVE-2020-3145**		
Improper Restriction of Operations within the Bounds of a Memory Buffer	16-Jul-20	9	Multiple vulnerabilities in the web-based management interface of the Cisco RV110W Wireless-N VPN Firewall, RV130 VPN Router, RV130W Wireless-N Multifunction VPN Router, and RV215W Wireless-N VPN Router could allow an authenticated, remote attacker to execute arbitrary code on an affected device. The vulnerabilities are due to improper validation of user-supplied data in the web-based management interface. An attacker could exploit these	N/A	O-CIS-RV13-190820/633

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			vulnerabilities by sending malicious HTTP requests to a targeted device. A successful exploit could allow the attacker to execute arbitrary code on the underlying operating system of the affected device as a high-privilege user. **CVE ID : CVE-2020-3146**		
rv215w_firmware					
Incorrect Authorization	16-Jul-20	4.3	A vulnerability in the web-based management interface of Cisco Small Business RV110W and RV215W Series Routers could allow an unauthenticated, remote attacker to download sensitive information from the device, which could include the device configuration. The vulnerability is due to improper authorization of an HTTP request. An attacker could exploit this vulnerability by accessing a specific URI on the web-based management interface of the router, but only after any valid user has opened a specific file on the device since the last reboot. A successful exploit would allow the attacker to view sensitive information, which should be restricted.	N/A	O-CIS-RV21-190820/634

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2020-3150		
Improper Authenticati on	16-Jul-20	7.5	A vulnerability in the web-based management interface of the Cisco RV110W Wireless-N VPN Firewall, RV130 VPN Router, RV130W Wireless-N Multifunction VPN Router, and RV215W Wireless-N VPN Router could allow an unauthenticated, remote attacker to bypass authentication and execute arbitrary commands with administrative commands on an affected device. The vulnerability is due to improper session management on affected devices. An attacker could exploit this vulnerability by sending a crafted HTTP request to the affected device. A successful exploit could allow the attacker to gain administrative access on the affected device. **CVE ID : CVE-2020-3144**	N/A	O-CIS-RV21-190820/635
Improper Restriction of Operations within the Bounds of a Memory Buffer	16-Jul-20	6.5	Multiple vulnerabilities in the web-based management interface of the Cisco RV110W Wireless-N VPN Firewall, RV130 VPN Router, RV130W Wireless-N Multifunction VPN Router, and RV215W Wireless-N VPN Router could allow an authenticated, remote	N/A	O-CIS-RV21-190820/636

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			attacker to execute arbitrary code on an affected device. The vulnerabilities are due to improper validation of user-supplied data in the web-based management interface. An attacker could exploit these vulnerabilities by sending malicious HTTP requests to a targeted device. A successful exploit could allow the attacker to execute arbitrary code on the underlying operating system of the affected device as a high-privilege user. **CVE ID : CVE-2020-3145**		
Improper Restriction of Operations within the Bounds of a Memory Buffer	16-Jul-20	9	Multiple vulnerabilities in the web-based management interface of the Cisco RV110W Wireless-N VPN Firewall, RV130 VPN Router, RV130W Wireless-N Multifunction VPN Router, and RV215W Wireless-N VPN Router could allow an authenticated, remote attacker to execute arbitrary code on an affected device. The vulnerabilities are due to improper validation of user-supplied data in the web-based management interface. An attacker could exploit these vulnerabilities by sending	N/A	O-CIS-RV21-190820/637

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			malicious HTTP requests to a targeted device. A successful exploit could allow the attacker to execute arbitrary code on the underlying operating system of the affected device as a high-privilege user. **CVE ID : CVE-2020-3146**		
ios_xe_sd-wan					
Improper Restriction of Operations within the Bounds of a Memory Buffer	31-Jul-20	10	A vulnerability in Cisco SD-WAN Solution Software could allow an unauthenticated, remote attacker to cause a buffer overflow on an affected device. The vulnerability is due to insufficient input validation. An attacker could exploit this vulnerability by sending crafted traffic to an affected device. A successful exploit could allow the attacker to gain access to information that they are not authorized to access, make changes to the system that they are not authorized to make, and execute commands on an affected system with privileges of the root user. **CVE ID : CVE-2020-3375**	N/A	O-CIS-IOS_-190820/638
Debian					
debian_linux					
NULL Pointer	29-Jul-20	4.3	In GNOME evolution-data-server before 3.35.91, a	N/A	O-DEB-DEBI-190820/639

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Dereference			malicious server can crash the mail client with a NULL pointer dereference by sending an invalid (e.g., minimal) CAPABILITY line on a connection attempt. This is related to imapx_free_capability and imapx_connect_to_server. **CVE ID : CVE-2020-16117**		
NULL Pointer Dereference	29-Jul-20	4.3	libssh 0.9.4 has a NULL pointer dereference in tftpserver.c if ssh_buffer_new returns NULL. **CVE ID : CVE-2020-16135**	N/A	O-DEB-DEBI-190820/640
Improper Neutralization of Special Elements in Output Used by a Downstream Component ('Injection')	17-Jul-20	4.3	evolution-data-server (eds) through 3.36.3 has a STARTTLS buffering issue that affects SMTP and POP3. When a server sends a "begin TLS" response, eds reads additional data and evaluates it in a TLS context, aka "response injection." **CVE ID : CVE-2020-14928**	https://bugzilla.suse.com/show_bug.cgi?id=1173910, https://gitlab.gnome.org/GNOME//evolution-data-server/commit/ba82be72cfd427b5d72ff21f929b3a6d8529c4df, https://lists.debian.org/debian-lts-announce/2020/07/msg00012.html	O-DEB-DEBI-190820/641
Improper Verification	29-Jul-20	4.4	GRUB2 fails to validate kernel signature when	https://lists.gnu.org/arch	O-DEB-DEBI-

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
of Cryptographic Signature			booted directly without shim, allowing secure boot to be bypassed. This only affects systems where the kernel signing certificate has been imported directly into the secure boot database and the GRUB image is booted directly without the use of shim. This issue affects GRUB2 version 2.04 and prior versions. **CVE ID : CVE-2020-15705**	ive/html/grub-devel/2020-07/msg00034.html, https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/ADV200011, https://security.netapp.com/advisory/ntap-20200731-0008/	190820/642
Concurrent Execution using Shared Resource with Improper Synchronization ('Race Condition')	29-Jul-20	4.4	GRUB2 contains a race condition in grub_script_function_create() leading to a use-after-free vulnerability which can be triggered by redefining a function whilst the same function is already executing, leading to arbitrary code execution and secure boot restriction bypass. This issue affects GRUB2 version 2.04 and prior versions. **CVE ID : CVE-2020-15706**	https://lists.gnu.org/archive/html/grub-devel/2020-07/msg00034.html, https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/ADV200011, https://security.netapp.com/advisory/ntap-20200731-0008/	O-DEB-DEBI-190820/643
Concurrent Execution using Shared	29-Jul-20	4.4	Integer overflows were discovered in the functions grub_cmd_initrd and	https://lists.gnu.org/archive/html/gru	O-DEB-DEBI-190820/644

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Resource with Improper Synchronization ('Race Condition')			grub_initrd_init in the efilinux component of GRUB2, as shipped in Debian, Red Hat, and Ubuntu (the functionality is not included in GRUB2 upstream), leading to a heap-based buffer overflow. These could be triggered by an extremely large number of arguments to the initrd command on 32-bit architectures, or a crafted filesystem with very large files on any architecture. An attacker could use this to execute arbitrary code and bypass UEFI Secure Boot restrictions. This issue affects GRUB2 version 2.04 and prior versions. **CVE ID : CVE-2020-15707**	b-devel/2020-07/msg00034.html, https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/ADV200011, https://security.netapp.com/advisory/ntap-20200731-0008/	
Out-of-bounds Read	21-Jul-20	5	LuaJit through 2.1.0-beta3 has an out-of-bounds read because __gc handler frame traversal is mishandled. **CVE ID : CVE-2020-15890**	N/A	O-DEB-DEBI-190820/645
Cleartext Transmission of Sensitive Information	27-Jul-20	4.3	KDE KMail 19.12.3 (aka 5.13.3) engages in unencrypted POP3 communication during times when the UI indicates that encryption is in use. **CVE ID : CVE-2020-15954**	N/A	O-DEB-DEBI-190820/646
Dlink					

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
dir-842_firmware					
Incorrect Implementation of Authentication Algorithm	23-Jul-20	5.8	This vulnerability allows network-adjacent attackers to bypass authentication on affected installations of D-Link DIR-842 3.13B05 routers. Authentication is not required to exploit this vulnerability. The specific flaw exists within the processing of HNAP GetCAPTCHAsetting requests. The issue results from the lack of proper handling of sessions. An attacker can leverage this vulnerability to execute arbitrary code in the context of the device. Was ZDI-CAN-10083. **CVE ID : CVE-2020-15632**	N/A	O-DLI-DIR--190820/647
dap-1860_firmware					
Improper Neutralization of Special Elements used in an OS Command ('OS Command Injection')	23-Jul-20	5.8	This vulnerability allows network-adjacent attackers to execute arbitrary code on affected installations of D-Link DAP-1860 1.04B03_HOTFIX WiFi extenders. Although authentication is required to exploit this vulnerability, the existing authentication mechanism can be bypassed. The specific flaw exists within the HNAP service, which listens on TCP port 80 by default. When parsing the	N/A	O-DLI-DAP--190820/648

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			SOAPAction header, the process does not properly validate a user-supplied string before using it to execute a system call. An attacker can leverage this vulnerability to execute code in the context of the device. Was ZDI-CAN-10084. **CVE ID : CVE-2020-15631**		
dsl-7740c_firmware					
Improper Neutralization of Special Elements used in an OS Command ('OS Command Injection')	22-Jul-20	4.6	D-Link DSL-7740C does not properly validate user input, which allows an authenticated LAN user to inject arbitrary command. **CVE ID : CVE-2020-12774**	N/A	O-DLI-DSL--190820/649
dap-1522_firmware					
Improper Authentication	22-Jul-20	5	An authentication-bypass issue was discovered on D-Link DAP-1522 devices 1.4x before 1.10b04Beta02. There exist a few pages that are directly accessible by any unauthorized user, e.g., logout.php and login.php. This occurs because of checking the value of NO_NEED_AUTH. If the value of NO_NEED_AUTH is 1, the user has direct access to the webpage without any authentication. By appending a query string	N/A	O-DLI-DAP--190820/650

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			NO_NEED_AUTH with the value of 1 to any protected URL, any unauthorized user can access the application directly, as demonstrated by bsc_lan.php?NO_NEED_AUTH=1. **CVE ID : CVE-2020-15896**		
D-link					
dir-867_firmware					
Authentication Bypass Using an Alternate Path or Channel	23-Jul-20	5.8	This vulnerability allows network-adjacent attackers to bypass authentication on affected installations of D-Link DIR-867, DIR-878, and DIR-882 routers with firmware 1.20B10_BETA. Authentication is not required to exploit this vulnerability. The specific flaw exists within the handling of HNAP requests. The issue results from incorrect string matching logic when accessing protected pages. An attacker can leverage this vulnerability to escalate privileges and execute code in the context of the router. Was ZDI-CAN-10835. **CVE ID : CVE-2020-15633**	N/A	O-D-L-DIR--190820/651
dir-882_firmware					
Authentication Bypass Using an	23-Jul-20	5.8	This vulnerability allows network-adjacent attackers to bypass	N/A	O-D-L-DIR--190820/652

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Alternate Path or Channel			authentication on affected installations of D-Link DIR-867, DIR-878, and DIR-882 routers with firmware 1.20B10_BETA. Authentication is not required to exploit this vulnerability. The specific flaw exists within the handling of HNAP requests. The issue results from incorrect string matching logic when accessing protected pages. An attacker can leverage this vulnerability to escalate privileges and execute code in the context of the router. Was ZDI-CAN-10835. **CVE ID : CVE-2020-15633**		
dap-1520_firmware					
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	22-Jul-20	7.5	An issue was discovered in apply.cgi on D-Link DAP-1520 devices before 1.10b04Beta02. Whenever a user performs a login action from the web interface, the request values are being forwarded to the ssi binary. On the login page, the web interface restricts the password input field to a fixed length of 15 characters. The problem is that validation is being done on the client side, hence it can be bypassed. When an attacker manages	N/A	O-D-L-DAP--190820/653

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			to intercept the login request (POST based) and tampers with the vulnerable parameter (log_pass), to a larger length, the request will be forwarded to the webserver. This results in a stack-based buffer overflow. A few other POST variables, (transferred as part of the login request) are also vulnerable: html_response_page and log_user. **CVE ID : CVE-2020-15892**		
dir-816l_firmware					
Improper Neutralization of Special Elements used in an OS Command ('OS Command Injection')	22-Jul-20	7.5	An issue was discovered on D-Link DIR-816L devices 2.x before 1.10b04Beta02. Universal Plug and Play (UPnP) is enabled by default on port 1900. An attacker can perform command injection by injecting a payload into the Search Target (ST) field of the SSDP M-SEARCH discover packet. **CVE ID : CVE-2020-15893**	N/A	O-D-L-DIR--190820/654
Information Exposure	22-Jul-20	5	An issue was discovered on D-Link DIR-816L devices 2.x before 1.10b04Beta02. There exists an exposed administration function in getcfg.php, which can be used to call various	N/A	O-D-L-DIR--190820/655

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			services. It can be utilized by an attacker to retrieve various sensitive information, such as admin login credentials, by setting the value of _POST_SERVICES in the query string to DEVICE.ACCOUNT. **CVE ID : CVE-2020-15894**		
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	22-Jul-20	4.3	An XSS issue was discovered on D-Link DIR-816L devices 2.x before 1.10b04Beta02. In the file webinc/js/info.php, no output filtration is applied to the RESULT parameter, before it's printed on the webpage. **CVE ID : CVE-2020-15895**	N/A	O-D-L-DIR--190820/656
dir-878_firmware					
Authentication Bypass Using an Alternate Path or Channel	23-Jul-20	5.8	This vulnerability allows network-adjacent attackers to bypass authentication on affected installations of D-Link DIR-867, DIR-878, and DIR-882 routers with firmware 1.20B10_BETA. Authentication is not required to exploit this vulnerability. The specific flaw exists within the handling of HNAP requests. The issue results from incorrect string matching logic when accessing protected pages. An attacker can leverage this vulnerability to	N/A	O-D-L-DIR--190820/657

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			escalate privileges and execute code in the context of the router. Was ZDI-CAN-10835. **CVE ID : CVE-2020-15633**		
Fedoraproject					
fedora					
Improper Neutralization of Special Elements in Output Used by a Downstream Component ('Injection')	17-Jul-20	4.3	evolution-data-server (eds) through 3.36.3 has a STARTTLS buffering issue that affects SMTP and POP3. When a server sends a "begin TLS" response, eds reads additional data and evaluates it in a TLS context, aka "response injection." **CVE ID : CVE-2020-14928**	https://bugzilla.suse.com/show_bug.cgi?id=1173910, https://gitlab.gnome.org/GNOME//evolution-data-server/commit/ba82be72cfd427b5d72ff21f929b3a6d8529c4df, https://lists.debian.org/debian-lts-announce/2020/07/msg00012.html	O-FED-FEDO-190820/658
Improper Input Validation	27-Jul-20	3.5	In FreeRDP less than or equal to 2.1.2, an integer overflow exists due to missing input sanitation in rdpegfx channel. All FreeRDP clients are affected. The input rectangles from the server are not checked against local surface coordinates and blindly accepted. A	https://github.com/FreeRDP/FreeRDP/security/advisories/GHSA-4r38-6hq7-j3j9	O-FED-FEDO-190820/659

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			malicious server can send data that will crash the client later on (invalid length arguments to a `memcpy`) This has been fixed in 2.2.0. As a workaround, stop using command line arguments /gfx, /gfx-h264 and /network:auto **CVE ID : CVE-2020-15103**		
Information Exposure	30-Jul-20	4.3	The Linux kernel through 5.7.11 allows remote attackers to make observations that help to obtain sensitive information about the internal state of the network RNG, aka CID-f227e3ec3b5c. This is related to drivers/char/random.c and kernel/time/timer.c. **CVE ID : CVE-2020-16166**	https://security.netapp.com/advisory/ntap-20200814-0004/	O-FED-FEDO-190820/660
Fortinet					
fortios					
Improper Authentication	24-Jul-20	7.5	An improper authentication vulnerability in SSL VPN in FortiOS 6.4.0, 6.2.0 to 6.2.3, 6.0.9 and below may result in a user being able to log in successfully without being prompted for the second factor of authentication (FortiToken) if they changed the case of their username.	N/A	O-FOR-FORT-190820/661

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2020-12812		
Google					
android					
Access of Resource Using Incompatible Type ('Type Confusion')	17-Jul-20	7.2	In createWithSurfaceParent of Client.cpp, there is a possible out of bounds write due to type confusion. This could lead to local escalation of privilege in the graphics server with no additional execution privileges needed. User interaction is not needed for exploitation.Product: AndroidVersions: Android-10Android ID: A-150226994 **CVE ID : CVE-2020-0226**	https://source.android.com/security/bulletin/2020-07-01	O-GOO-ANDR-190820/662
Incorrect Default Permissions	17-Jul-20	7.2	In onCommand of CompanionDeviceManagerService.java, there is a possible permissions bypass due to a missing permission check. This could lead to local escalation of privilege allowing background data usage or launching from the background, 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-129476618	https://source.android.com/security/bulletin/2020-07-01	O-GOO-ANDR-190820/663

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2020-0227		
Information Exposure	17-Jul-20	5	There is an improper configuration of recorder related service. Product: AndroidVersions: Android SoCAndroid ID: A-156333723 **CVE ID : CVE-2020-0228**	https://source.android.com/security/bulletin/2020-07-01	O-GOO-ANDR-190820/664
Out-of-bounds Write	17-Jul-20	7.5	There is a possible out of bounds write due to an incorrect bounds check. Product: AndroidVersions: Android SoCAndroid ID: A-156337262 **CVE ID : CVE-2020-0230**	https://source.android.com/security/bulletin/2020-07-01	O-GOO-ANDR-190820/665
Out-of-bounds Write	17-Jul-20	7.5	There is a possible out of bounds write due to an incorrect bounds check. Product: AndroidVersions: Android SoCAndroid ID: A-156333727 **CVE ID : CVE-2020-0231**	https://source.android.com/security/bulletin/2020-07-01	O-GOO-ANDR-190820/666
Incorrect Default Permissions	17-Jul-20	2.1	In getUiccCardsInfo of PhoneInterfaceManager.java, there is a possible permissions bypass due to improper input validation. This could lead to local information disclosure with no additional execution privileges needed. User interaction is not needed for exploitation.Product: AndroidVersions: Android-10Android ID: A-146570216 **CVE ID : CVE-2020-0107**	https://source.android.com/security/bulletin/2020-07-01	O-GOO-ANDR-190820/667

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Out-of-bounds Write	17-Jul-20	4.6	In notifyErrorForPendingRequests of QCamera3HWI.cpp, there is a possible out of bounds write due to a heap buffer overflow. This could lead to local escalation of privilege with no additional execution privileges needed. User interaction is not needed for exploitation.Product: AndroidVersions: Android-10Android ID: A-149995442 **CVE ID : CVE-2020-0120**	https://source.android.com/security/bulletin/pixel/2020-06-01	O-GOO-ANDR-190820/668
Incorrect Default Permissions	17-Jul-20	7.2	In the permission declaration for com.google.android.providers.gsf.permission.WRITE_GSERVICES in AndroidManifest.xml, there is a possible permissions bypass. This could lead to local escalation of privilege with System execution privileges needed. User interaction is not needed for exploitation.Product: AndroidVersions: Android-8.0 Android-8.1 Android-9 Android-10Android ID: A-147247775 **CVE ID : CVE-2020-0122**	https://source.android.com/security/bulletin/2020-07-01	O-GOO-ANDR-190820/669
Access of Resource Using Incompatible	17-Jul-20	10	In FastKeyAccumulator::GetKeysSlow of keys.cc, there is a possible out of bounds	https://source.android.com/security/bulletin/202	O-GOO-ANDR-190820/670

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Type ('Type Confusion')			write due to type confusion. This could lead to remote code execution when processing a proxy configuration 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-147664838 **CVE ID : CVE-2020-0224**	0-07-01	
Out-of-bounds Write	17-Jul-20	10	In a2dp_vendor_ldac_decoder_decode_packet of a2dp_vendor_ldac_decoder.cc, there is a possible out of bounds write due to a missing bounds check. This could lead to remote code execution with no additional execution privileges needed. User interaction is not needed for exploitation.Product: AndroidVersions: Android-10Android ID: A-142546668 **CVE ID : CVE-2020-0225**	https://source.android.com/security/bulletin/2020-07-01	O-GOO-ANDR-190820/671
Concurrent Execution using Shared Resource with Improper Synchronization ('Race Condition')	17-Jul-20	4.4	In cdev_get of char_dev.c, there is a possible use-after-free due to a race condition. This could lead to local escalation of privilege with System execution privileges needed. User interaction is not needed for	https://source.android.com/security/bulletin/pixel/2020-06-01	O-GOO-ANDR-190820/672

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			exploitation.Product: AndroidVersions: Android-10Android ID: A-153467744 **CVE ID : CVE-2020-0305**		
Incorrect Authorization	22-Jul-20	4.3	Insufficient policy enforcement in WebView in Google Chrome on Android prior to 83.0.4103.106 allowed a remote attacker to bypass site isolation via a crafted HTML page. **CVE ID : CVE-2020-6506**	N/A	O-GOO-ANDR-190820/673
Grandstream					
gwn7000_firmware					
Improper Neutralization of Special Elements used in an OS Command ('OS Command Injection')	17-Jul-20	9	Grandstream GWN7000 firmware version 1.0.9.4 and below allows authenticated remote users to modify the system's crontab via undocumented API. An attacker can use this functionality to execute arbitrary OS commands on the router. **CVE ID : CVE-2020-5756**	https://www.tenable.com/security/research/tra-2020-41	O-GRA-GWN7-190820/674
ucm6204_firmware					
Improper Neutralization of Special Elements used in an OS Command ('OS Command Injection')	17-Jul-20	10	Grandstream UCM6200 series firmware version 1.0.20.23 and below is vulnerable to OS command injection via HTTP. An authenticated remote attacker can bypass command injection mitigations and execute	https://www.tenable.com/security/research/tra-2020-42	O-GRA-UCM6-190820/675

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			commands as the root user by sending a crafted HTTP POST to the UCM's "New" HTTPS API. **CVE ID : CVE-2020-5757**		
Improper Neutralization of Special Elements used in an OS Command ('OS Command Injection')	17-Jul-20	9	Grandstream UCM6200 series firmware version 1.0.20.23 and below is vulnerable to OS command injection via HTTP. An authenticated remote attacker can execute commands as the root user by sending a crafted HTTP GET to the UCM's "Old" HTTPS API. **CVE ID : CVE-2020-5758**	https://www.tenable.com/security/research/tra-2020-42	O-GRA-UCM6-190820/676
Improper Neutralization of Special Elements used in an OS Command ('OS Command Injection')	17-Jul-20	10	Grandstream UCM6200 series firmware version 1.0.20.23 and below is vulnerable to OS command injection via SSH. An authenticated remote attacker can execute commands as the root user by issuing a specially crafted "unset" command. **CVE ID : CVE-2020-5759**	https://www.tenable.com/security/research/tra-2020-42	O-GRA-UCM6-190820/677
ht801_firmware					
Improper Neutralization of Special Elements used in an OS Command ('OS Command Injection')	29-Jul-20	9.3	Grandstream HT800 series firmware version 1.0.17.5 and below is vulnerable to an OS command injection vulnerability. Unauthenticated remote attackers can execute arbitrary commands as root by crafting a special configuration file and	N/A	O-GRA-HT80-190820/678

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			sending a crafted SIP message. **CVE ID : CVE-2020-5760**		
Loop with Unreachable Exit Condition ('Infinite Loop')	29-Jul-20	7.8	Grandstream HT800 series firmware version 1.0.17.5 and below is vulnerable to CPU exhaustion due to an infinite loop in the TR-069 service. Unauthenticated remote attackers can trigger this case by sending a one character TCP message to the TR-069 service. **CVE ID : CVE-2020-5761**	N/A	O-GRA-HT80-190820/679
NULL Pointer Dereference	29-Jul-20	5	Grandstream HT800 series firmware version 1.0.17.5 and below is vulnerable to a denial of service attack against the TR-069 service. An unauthenticated remote attacker can stop the service due to a NULL pointer dereference in the TR-069 service. This condition is triggered due to mishandling of the HTTP Authentication field. **CVE ID : CVE-2020-5762**	N/A	O-GRA-HT80-190820/680
Inadequate Encryption Strength	29-Jul-20	9	Grandstream HT800 series firmware version 1.0.17.5 and below contain a backdoor in the SSH service. An authenticated remote attacker can obtain a root shell by correctly answering a challenge prompt. **CVE ID : CVE-2020-5763**	N/A	O-GRA-HT80-190820/681

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
ht802_firmware					
Improper Neutralization of Special Elements used in an OS Command ('OS Command Injection')	29-Jul-20	9.3	Grandstream HT800 series firmware version 1.0.17.5 and below is vulnerable to an OS command injection vulnerability. Unauthenticated remote attackers can execute arbitrary commands as root by crafting a special configuration file and sending a crafted SIP message. **CVE ID : CVE-2020-5760**	N/A	O-GRA-HT80-190820/682
Loop with Unreachable Exit Condition ('Infinite Loop')	29-Jul-20	7.8	Grandstream HT800 series firmware version 1.0.17.5 and below is vulnerable to CPU exhaustion due to an infinite loop in the TR-069 service. Unauthenticated remote attackers can trigger this case by sending a one character TCP message to the TR-069 service. **CVE ID : CVE-2020-5761**	N/A	O-GRA-HT80-190820/683
NULL Pointer Dereference	29-Jul-20	5	Grandstream HT800 series firmware version 1.0.17.5 and below is vulnerable to a denial of service attack against the TR-069 service. An unauthenticated remote attacker can stop the service due to a NULL pointer dereference in the TR-069 service. This condition is triggered due to mishandling of the HTTP Authentication field.	N/A	O-GRA-HT80-190820/684

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2020-5762		
Inadequate Encryption Strength	29-Jul-20	9	Grandstream HT800 series firmware version 1.0.17.5 and below contain a backdoor in the SSH service. An authenticated remote attacker can obtain a root shell by correctly answering a challenge prompt. **CVE ID : CVE-2020-5763**	N/A	O-GRA-HT80-190820/685
ht812_firmware					
Improper Neutralization of Special Elements used in an OS Command ('OS Command Injection')	29-Jul-20	9.3	Grandstream HT800 series firmware version 1.0.17.5 and below is vulnerable to an OS command injection vulnerability. Unauthenticated remote attackers can execute arbitrary commands as root by crafting a special configuration file and sending a crafted SIP message. **CVE ID : CVE-2020-5760**	N/A	O-GRA-HT81-190820/686
Loop with Unreachable Exit Condition ('Infinite Loop')	29-Jul-20	7.8	Grandstream HT800 series firmware version 1.0.17.5 and below is vulnerable to CPU exhaustion due to an infinite loop in the TR-069 service. Unauthenticated remote attackers can trigger this case by sending a one character TCP message to the TR-069 service. **CVE ID : CVE-2020-5761**	N/A	O-GRA-HT81-190820/687
NULL Pointer	29-Jul-20	5	Grandstream HT800 series firmware version 1.0.17.5	N/A	O-GRA-HT81-

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Dereference			and below is vulnerable to a denial of service attack against the TR-069 service. An unauthenticated remote attacker can stop the service due to a NULL pointer dereference in the TR-069 service. This condition is triggered due to mishandling of the HTTP Authentication field. **CVE ID : CVE-2020-5762**		190820/688
Inadequate Encryption Strength	29-Jul-20	9	Grandstream HT800 series firmware version 1.0.17.5 and below contain a backdoor in the SSH service. An authenticated remote attacker can obtain a root shell by correctly answering a challenge prompt. **CVE ID : CVE-2020-5763**	N/A	O-GRA-HT81-190820/689
ht814_firmware					
Improper Neutralization of Special Elements used in an OS Command ('OS Command Injection')	29-Jul-20	9.3	Grandstream HT800 series firmware version 1.0.17.5 and below is vulnerable to an OS command injection vulnerability. Unauthenticated remote attackers can execute arbitrary commands as root by crafting a special configuration file and sending a crafted SIP message. **CVE ID : CVE-2020-5760**	N/A	O-GRA-HT81-190820/690
Loop with Unreachable Exit	29-Jul-20	7.8	Grandstream HT800 series firmware version 1.0.17.5 and below is vulnerable to	N/A	O-GRA-HT81-190820/691

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Condition ('Infinite Loop')			CPU exhaustion due to an infinite loop in the TR-069 service. Unauthenticated remote attackers can trigger this case by sending a one character TCP message to the TR-069 service. **CVE ID : CVE-2020-5761**		
NULL Pointer Dereference	29-Jul-20	5	Grandstream HT800 series firmware version 1.0.17.5 and below is vulnerable to a denial of service attack against the TR-069 service. An unauthenticated remote attacker can stop the service due to a NULL pointer dereference in the TR-069 service. This condition is triggered due to mishandling of the HTTP Authentication field. **CVE ID : CVE-2020-5762**	N/A	O-GRA-HT81-190820/692
Inadequate Encryption Strength	29-Jul-20	9	Grandstream HT800 series firmware version 1.0.17.5 and below contain a backdoor in the SSH service. An authenticated remote attacker can obtain a root shell by correctly answering a challenge prompt. **CVE ID : CVE-2020-5763**	N/A	O-GRA-HT81-190820/693
ht818_firmware					
Improper Neutralization of Special Elements used in an OS	29-Jul-20	9.3	Grandstream HT800 series firmware version 1.0.17.5 and below is vulnerable to an OS command injection vulnerability.	N/A	O-GRA-HT81-190820/694

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Command ('OS Command Injection')			Unauthenticated remote attackers can execute arbitrary commands as root by crafting a special configuration file and sending a crafted SIP message. **CVE ID : CVE-2020-5760**		
Loop with Unreachable Exit Condition ('Infinite Loop')	29-Jul-20	7.8	Grandstream HT800 series firmware version 1.0.17.5 and below is vulnerable to CPU exhaustion due to an infinite loop in the TR-069 service. Unauthenticated remote attackers can trigger this case by sending a one character TCP message to the TR-069 service. **CVE ID : CVE-2020-5761**	N/A	O-GRA-HT81-190820/695
NULL Pointer Dereference	29-Jul-20	5	Grandstream HT800 series firmware version 1.0.17.5 and below is vulnerable to a denial of service attack against the TR-069 service. An unauthenticated remote attacker can stop the service due to a NULL pointer dereference in the TR-069 service. This condition is triggered due to mishandling of the HTTP Authentication field. **CVE ID : CVE-2020-5762**	N/A	O-GRA-HT81-190820/696
Inadequate Encryption Strength	29-Jul-20	9	Grandstream HT800 series firmware version 1.0.17.5 and below contain a backdoor in the SSH service. An authenticated	N/A	O-GRA-HT81-190820/697

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			remote attacker can obtain a root shell by correctly answering a challenge prompt. **CVE ID : CVE-2020-5763**		
ht813_firmware					
Improper Neutralization of Special Elements used in an OS Command ('OS Command Injection')	29-Jul-20	9.3	Grandstream HT800 series firmware version 1.0.17.5 and below is vulnerable to an OS command injection vulnerability. Unauthenticated remote attackers can execute arbitrary commands as root by crafting a special configuration file and sending a crafted SIP message. **CVE ID : CVE-2020-5760**	N/A	O-GRA-HT81-190820/698
Loop with Unreachable Exit Condition ('Infinite Loop')	29-Jul-20	7.8	Grandstream HT800 series firmware version 1.0.17.5 and below is vulnerable to CPU exhaustion due to an infinite loop in the TR-069 service. Unauthenticated remote attackers can trigger this case by sending a one character TCP message to the TR-069 service. **CVE ID : CVE-2020-5761**	N/A	O-GRA-HT81-190820/699
NULL Pointer Dereference	29-Jul-20	5	Grandstream HT800 series firmware version 1.0.17.5 and below is vulnerable to a denial of service attack against the TR-069 service. An unauthenticated remote attacker can stop the service due to a NULL	N/A	O-GRA-HT81-190820/700

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			pointer dereference in the TR-069 service. This condition is triggered due to mishandling of the HTTP Authentication field. **CVE ID : CVE-2020-5762**		
Inadequate Encryption Strength	29-Jul-20	9	Grandstream HT800 series firmware version 1.0.17.5 and below contain a backdoor in the SSH service. An authenticated remote attacker can obtain a root shell by correctly answering a challenge prompt. **CVE ID : CVE-2020-5763**	N/A	O-GRA-HT81-190820/701
ucm6202_firmware					
Improper Neutralization of Special Elements used in an OS Command ('OS Command Injection')	17-Jul-20	10	Grandstream UCM6200 series firmware version 1.0.20.23 and below is vulnerable to OS command injection via SSH. An authenticated remote attacker can execute commands as the root user by issuing a specially crafted "unset" command. **CVE ID : CVE-2020-5759**	https://www.tenable.com/security/research/tra-2020-42	O-GRA-UCM6-190820/702
Improper Neutralization of Special Elements used in an OS Command ('OS Command Injection')	17-Jul-20	10	Grandstream UCM6200 series firmware version 1.0.20.23 and below is vulnerable to OS command injection via HTTP. An authenticated remote attacker can bypass command injection mitigations and execute commands as the root user by sending a crafted HTTP	https://www.tenable.com/security/research/tra-2020-42	O-GRA-UCM6-190820/703

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			POST to the UCM's "New" HTTPS API. **CVE ID : CVE-2020-5757**		
Improper Neutralization of Special Elements used in an OS Command ('OS Command Injection')	17-Jul-20	9	Grandstream UCM6200 series firmware version 1.0.20.23 and below is vulnerable to OS command injection via HTTP. An authenticated remote attacker can execute commands as the root user by sending a crafted HTTP GET to the UCM's "Old" HTTPS API. **CVE ID : CVE-2020-5758**	https://www.tenable.com/security/research/tra-2020-42	O-GRA-UCM6-190820/704
ucm6208_firmware					
Improper Neutralization of Special Elements used in an OS Command ('OS Command Injection')	17-Jul-20	10	Grandstream UCM6200 series firmware version 1.0.20.23 and below is vulnerable to OS command injection via HTTP. An authenticated remote attacker can bypass command injection mitigations and execute commands as the root user by sending a crafted HTTP POST to the UCM's "New" HTTPS API. **CVE ID : CVE-2020-5757**	https://www.tenable.com/security/research/tra-2020-42	O-GRA-UCM6-190820/705
Improper Neutralization of Special Elements used in an OS Command ('OS Command Injection')	17-Jul-20	9	Grandstream UCM6200 series firmware version 1.0.20.23 and below is vulnerable to OS command injection via HTTP. An authenticated remote attacker can execute commands as the root user by sending a crafted HTTP	https://www.tenable.com/security/research/tra-2020-42	O-GRA-UCM6-190820/706

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			GET to the UCM's "Old" HTTPS API. **CVE ID : CVE-2020-5758**		
Improper Neutralization of Special Elements used in an OS Command ('OS Command Injection')	17-Jul-20	10	Grandstream UCM6200 series firmware version 1.0.20.23 and below is vulnerable to OS command injection via SSH. An authenticated remote attacker can execute commands as the root user by issuing a specially crafted "unset" command. **CVE ID : CVE-2020-5759**	https://www.tenable.com/security/research/tra-2020-42	O-GRA-UCM6-190820/707
grundfos					
cim_500_firmware					
Missing Authentication for Critical Function	17-Jul-20	5	Grundfos CIM 500 before v06.16.00 responds to unauthenticated requests for password storage files. **CVE ID : CVE-2020-10605**	https://us-cert.cisa.gov/ics/advisories/icsa-20-189-01	O-GRU-CIM_-190820/708
Huawei					
cloudengine_6800_firmware					
Information Exposure	17-Jul-20	2.1	There is a information leak vulnerability in some Huawei products, and it could allow a local attacker to get information. The vulnerability is due to the improper management of the username. An attacker with the ability to access the device and cause the username information leak. Affected product versions include: CloudEngine 12800 versions	https://www.huawei.com/en/psirt/security-advisories/huawei-sa-20200715-03-informationleak-en	O-HUA-CLOU-190820/709

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			V200R002C50SPC800, V200R003C00SPC810, V200R005C00SPC800, V200R005C10SPC800, V200R019C00SPC800; CloudEngine 5800 versions V200R002C50SPC800, V200R003C00SPC810, V200R005C00SPC800, V200R005C10SPC800, V200R019C00SPC800; CloudEngine 6800 versions V200R002C50SPC800, V200R003C00SPC810, V200R005C00SPC800, V200R005C10SPC800, V200R005C20SPC800, V200R019C00SPC800; CloudEngine 7800 versions V200R002C50SPC800, V200R003C00SPC810, V200R005C00SPC800, V200R005C10SPC800, V200R019C00SPC800 **CVE ID : CVE-2020-9102**		
mate_30_pro_firmware					
N/A	18-Jul-20	4.3	Huawei Mate 30 Pro smartphones with versions earlier than 10.1.0.150(C00E136R5P3) have an improper authorization vulnerability. The system does not properly restrict the use of system service by applications, the attacker should trick the	https://www.huawei.com/en/psirt/security-advisories/huawei-sa-20200715-05-smartphone-en	O-HUA-MATE-190820/710

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			user into installing a malicious application, successful exploit could cause a denial of audio service. **CVE ID : CVE-2020-9256**		
cloudengine_5800_firmware					
Information Exposure	17-Jul-20	2.1	There is a information leak vulnerability in some Huawei products, and it could allow a local attacker to get information. The vulnerability is due to the improper management of the username. An attacker with the ability to access the device and cause the username information leak. Affected product versions include: CloudEngine 12800 versions V200R002C50SPC800, V200R003C00SPC810, V200R005C00SPC800, V200R005C10SPC800, V200R019C00SPC800; CloudEngine 5800 versions V200R002C50SPC800, V200R003C00SPC810, V200R005C00SPC800, V200R005C10SPC800, V200R019C00SPC800; CloudEngine 6800 versions V200R002C50SPC800, V200R003C00SPC810, V200R005C00SPC800, V200R005C10SPC800,	https://www.huawei.com/en/psirt/security-advisories/huawei-sa-20200715-03-informationleak-en	O-HUA-CLOU-190820/711

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			V200R005C20SPC800, V200R019C00SPC800; CloudEngine 7800 versions V200R002C50SPC800, V200R003C00SPC810, V200R005C00SPC800, V200R005C10SPC800, V200R019C00SPC800 **CVE ID : CVE-2020-9102**		
cloudengine_7800_firmware					
Information Exposure	17-Jul-20	2.1	There is a information leak vulnerability in some Huawei products, and it could allow a local attacker to get information. The vulnerability is due to the improper management of the username. An attacker with the ability to access the device and cause the username information leak. Affected product versions include: CloudEngine 12800 versions V200R002C50SPC800, V200R003C00SPC810, V200R005C00SPC800, V200R005C10SPC800, V200R019C00SPC800; CloudEngine 5800 versions V200R002C50SPC800, V200R003C00SPC810, V200R005C00SPC800, V200R005C10SPC800, V200R019C00SPC800; CloudEngine 6800 versions	https://www.huawei.com/en/psirt/security-advisories/huawei-sa-20200715-03-informationleak-en	O-HUA-CLOU-190820/712

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			V200R002C50SPC800, V200R003C00SPC810, V200R005C00SPC800, V200R005C10SPC800, V200R005C20SPC800, V200R019C00SPC800; CloudEngine 7800 versions V200R002C50SPC800, V200R003C00SPC810, V200R005C00SPC800, V200R005C10SPC800, V200R019C00SPC800 **CVE ID : CVE-2020-9102**		
moana-al00b_firmware					
Missing Initialization of Resource	17-Jul-20	4.3	Huawei Smart Phones Moana-AL00B with versions earlier than 10.1.0.166 have a missing initialization of resource vulnerability. An attacker tricks the user into installing then running a crafted application. Due to improper initialization of specific parameters, successful exploit of this vulnerability may cause device exceptions. **CVE ID : CVE-2020-9227**	https://www.huawei.com/en/psirt/security-advisories/huawei-sa-20200715-09-smartphone-en	O-HUA-MOAN-190820/713
magic2_firmware					
Improper Limitation of a Pathname to a Restricted Directory ('Path Traversal')	17-Jul-20	2.1	HUAWEI Mate 20 versions earlier than 10.1.0.160(C00E160R3P8), HUAWEI Mate 20 X versions earlier than 10.1.0.135(C00E135R2P8), HUAWEI Mate 20 RS versions earlier than	https://www.huawei.com/en/psirt/security-advisories/huawei-sa-20200715-07-	O-HUA-MAGI-190820/714

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			10.1.0.160(C786E160R3P8), and Honor Magic2 smartphones versions earlier than 10.1.0.160(C00E160R2P11) have a path traversal vulnerability. The system does not sufficiently validate certain pathname from certain process, successful exploit could allow the attacker write files to a crafted path. **CVE ID : CVE-2020-9252**	smartphone-en	
ips_module_firmware					
Out-of-bounds Write	18-Jul-20	3.3	There is an out-of-bounds write vulnerability in some products. An unauthenticated attacker crafts malformed packets with specific parameter and sends the packets to the affected products. Due to insufficient validation of packets, which may be exploited to cause the process reboot. Affected product versions include: IPS Module versions V500R005C00, V500R005C10; NGFW Module versions V500R005C00, V500R005C10; Secospace USG6300 versions V500R001C30, V500R001C60, V500R005C00, V500R005C10; Secospace USG6500 versions	https://www.huawei.com/en/psirt/security-advisories/huawei-sa-20200715-01-outofbounds write-en	O-HUA-IPS_-190820/715

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			V500R001C30, V500R001C60, V500R005C00, V500R005C10; Secospace USG6600 versions V500R001C30, V500R001C60, V500R005C00, V500R005C10; USG9500 versions V500R001C30, V500R001C60, V500R005C00, V500R005C10 **CVE ID : CVE-2020-9101**		
cloudengine_12800_firmware					
Information Exposure	17-Jul-20	2.1	There is a information leak vulnerability in some Huawei products, and it could allow a local attacker to get information. The vulnerability is due to the improper management of the username. An attacker with the ability to access the device and cause the username information leak. Affected product versions include: CloudEngine 12800 versions V200R002C50SPC800, V200R003C00SPC810, V200R005C00SPC800, V200R005C10SPC800, V200R019C00SPC800; CloudEngine 5800 versions V200R002C50SPC800, V200R003C00SPC810, V200R005C00SPC800,	https://www.huawei.com/en/psirt/security-advisories/huawei-sa-20200715-03-informationleak-en	O-HUA-CLOU-190820/716

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			V200R005C10SPC800, V200R019C00SPC800; CloudEngine 6800 versions V200R002C50SPC800, V200R003C00SPC810, V200R005C00SPC800, V200R005C10SPC800, V200R005C20SPC800, V200R019C00SPC800; CloudEngine 7800 versions V200R002C50SPC800, V200R003C00SPC810, V200R005C00SPC800, V200R005C10SPC800, V200R019C00SPC800 **CVE ID : CVE-2020-9102**		
honor_v30_firmware					
Improper Authentication	17-Jul-20	4.3	Huawei Honor V30 smartphones with versions earlier than 10.1.0.212(C00E210R5P1) have an improper authentication vulnerability. The system does not sufficiently validate certain parameter passed from the bottom level, the attacker should trick the user into installing a malicious application and control the bottom level, successful exploit could cause information disclosure. **CVE ID : CVE-2020-9259**	https://www.huawei.com/en/psirt/security-advisories/huawei-sa-20200715-02-smartphone-en	O-HUA-HONO-190820/717
secospace_usg6300_firmware					
Out-of-	18-Jul-20	3.3	There is an out-of-bounds	https://ww	O-HUA-SECO-

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
bounds Write			write vulnerability in some products. An unauthenticated attacker crafts malformed packets with specific parameter and sends the packets to the affected products. Due to insufficient validation of packets, which may be exploited to cause the process reboot. Affected product versions include: IPS Module versions V500R005C00, V500R005C10; NGFW Module versions V500R005C00, V500R005C10; Secospace USG6300 versions V500R001C30, V500R001C60, V500R005C00, V500R005C10; Secospace USG6500 versions V500R001C30, V500R001C60, V500R005C00, V500R005C10; Secospace USG6600 versions V500R001C30, V500R001C60, V500R005C00, V500R005C10; USG9500 versions V500R001C30, V500R001C60, V500R005C00, V500R005C10 **CVE ID : CVE-2020-9101**	w.huawei.com/en/psirt/security-advisories/huawei-sa-20200715-01-outofbounds write-en	190820/718
secospace_usg6500_firmware					
Out-of-	18-Jul-20	3.3	There is an out-of-bounds	https://ww	O-HUA-SECO-

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
bounds Write			write vulnerability in some products. An unauthenticated attacker crafts malformed packets with specific parameter and sends the packets to the affected products. Due to insufficient validation of packets, which may be exploited to cause the process reboot. Affected product versions include: IPS Module versions V500R005C00, V500R005C10; NGFW Module versions V500R005C00, V500R005C10; Secospace USG6300 versions V500R001C30, V500R001C60, V500R005C00, V500R005C10; Secospace USG6500 versions V500R001C30, V500R001C60, V500R005C00, V500R005C10; Secospace USG6600 versions V500R001C30, V500R001C60, V500R005C00, V500R005C10; USG9500 versions V500R001C30, V500R001C60, V500R005C00, V500R005C10 **CVE ID : CVE-2020-9101**	w.huawei.com/en/psirt/security-advisories/huawei-sa-20200715-01-outofbounds write-en	190820/719
secospace_usg6600_firmware					
Out-of-	18-Jul-20	3.3	There is an out-of-bounds	https://ww	O-HUA-SECO-

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
bounds Write			write vulnerability in some products. An unauthenticated attacker crafts malformed packets with specific parameter and sends the packets to the affected products. Due to insufficient validation of packets, which may be exploited to cause the process reboot. Affected product versions include: IPS Module versions V500R005C00, V500R005C10; NGFW Module versions V500R005C00, V500R005C10; Secospace USG6300 versions V500R001C30, V500R001C60, V500R005C00, V500R005C10; Secospace USG6500 versions V500R001C30, V500R001C60, V500R005C00, V500R005C10; Secospace USG6600 versions V500R001C30, V500R001C60, V500R005C00, V500R005C10; USG9500 versions V500R001C30, V500R001C60, V500R005C00, V500R005C10 **CVE ID : CVE-2020-9101**	w.huawei.com/en/psirt/security-advisories/huawei-sa-20200715-01-outofbounds write-en	190820/720
p30_pro_firmware					
Improper	17-Jul-20	6.8	HUAWEI P30 Pro	https://ww	O-HUA-P30_-

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Neutralization of Special Elements in Output Used by a Downstream Component ('Injection')			smartphones with versions earlier than 10.1.0.123(C432E19R2P5 patch02), versions earlier than 10.1.0.126(C10E11R5P1), and versions earlier than 10.1.0.160(C00E160R2P8) have a logic check error vulnerability. A logic error occurs when the software checking the size of certain parameter, the attacker should trick the user into installing a malicious application, successful exploit may cause code execution. **CVE ID : CVE-2020-9254**	w.huawei.com/en/psirt/security-advisories/huawei-sa-20200715-04-smartphone-en	190820/721
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	17-Jul-20	6.8	HUAWEI P30 Pro smartphones with versions earlier than 10.1.0.123(C432E19R2P5 patch02), versions earlier than 10.1.0.126(C10E11R5P1), and versions earlier than 10.1.0.160(C00E160R2P8) have a buffer overflow vulnerability. The software access data past the end, or before the beginning, of the intended buffer when handling certain operations of certificate, the attacker should trick the user into installing a malicious application, successful exploit may cause code execution.	https://www.huawei.com/en/psirt/security-advisories/huawei-sa-20200715-03-smartphone-en	O-HUA-P30_-190820/722

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2020-9257		
p30_firmware					
Information Exposure	27-Jul-20	4.3	HUAWEI P30 smart phones with versions earlier than 10.1.0.160(C00E160R2P11) have an information exposure vulnerability. The system does not properly authenticate the application that access a specified interface. Attackers can trick users into installing malicious software to exploit this vulnerability and obtain some information about the device. Successful exploit may cause information disclosure. **CVE ID : CVE-2020-9077**	N/A	O-HUA-P30_-190820/723
Improper Input Validation	31-Jul-20	3.3	HUAWEI P30 smartphones with versions earlier than 10.1.0.160(C00E160R2P11) have a denial of service vulnerability. A module does not deal with mal-crafted messages and it leads to memory leak. Attackers can exploit this vulnerability to make the device denial of service.Affected product versions include: HUAWEI P30 versions Versions earlier than 10.1.0.160(C00E160R2P11). **CVE ID : CVE-2020-9249**	N/A	O-HUA-P30_-190820/724

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Improper Authenticati on	27-Jul-20	2.1	HUAWEI Mate 20 smartphones with versions earlier than 10.1.0.160(C00E160R2P11) have an improper authorization vulnerability. The software does not properly restrict certain operation in certain scenario, the attacker should do certain configuration before the user turns on student mode function. Successful exploit could allow the attacker to bypass the limit of student mode function. Affected product versions include: HUAWEI Mate 20 versions Versions earlier than 10.1.0.160(C00E160R3P8). **CVE ID : CVE-2020-9251**	N/A	O-HUA-P30_-190820/725
honor_10_firmware					
Improper Input Validation	17-Jul-20	4.3	Huawei Honor 10 smartphones with versions earlier than 10.0.0.178(C00E178R1P4) have a denial of service vulnerability. Certain service in the system does not sufficiently validate certain parameter which is received, the attacker should trick the user into installing a malicious application, successful exploit could cause a denial of service condition.	https://www.huawei.com/en/psirt/security-advisories/huawei-sa-20200715-06-smartphone-en	O-HUA-HONO-190820/726

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2020-9255		
mate_20_x_firmware					
Improper Limitation of a Pathname to a Restricted Directory ('Path Traversal')	17-Jul-20	2.1	HUAWEI Mate 20 versions earlier than 10.1.0.160(C00E160R3P8), HUAWEI Mate 20 X versions earlier than 10.1.0.135(C00E135R2P8), HUAWEI Mate 20 RS versions earlier than 10.1.0.160(C786E160R3P8), and Honor Magic2 smartphones versions earlier than 10.1.0.160(C00E160R2P11) have a path traversal vulnerability. The system does not sufficiently validate certain pathname from certain process, successful exploit could allow the attacker write files to a crafted path. **CVE ID : CVE-2020-9252**	https://www.huawei.com/en/psirt/security-advisories/huawei-sa-20200715-07-smartphone-en	O-HUA-MATE-190820/727
mate_20_firmware					
Improper Limitation of a Pathname to a Restricted Directory ('Path Traversal')	17-Jul-20	2.1	HUAWEI Mate 20 versions earlier than 10.1.0.160(C00E160R3P8), HUAWEI Mate 20 X versions earlier than 10.1.0.135(C00E135R2P8), HUAWEI Mate 20 RS versions earlier than 10.1.0.160(C786E160R3P8), and Honor Magic2 smartphones versions earlier than 10.1.0.160(C00E160R2P11) have a path traversal vulnerability. The system	https://www.huawei.com/en/psirt/security-advisories/huawei-sa-20200715-07-smartphone-en	O-HUA-MATE-190820/728

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			does not sufficiently validate certain pathname from certain process, successful exploit could allow the attacker write files to a crafted path. **CVE ID : CVE-2020-9252**		
ngfw_module_firmware					
Out-of-bounds Write	18-Jul-20	3.3	There is an out-of-bounds write vulnerability in some products. An unauthenticated attacker crafts malformed packets with specific parameter and sends the packets to the affected products. Due to insufficient validation of packets, which may be exploited to cause the process reboot. Affected product versions include: IPS Module versions V500R005C00, V500R005C10; NGFW Module versions V500R005C00, V500R005C10; Secospace USG6300 versions V500R001C30, V500R001C60, V500R005C00, V500R005C10; Secospace USG6500 versions V500R001C30, V500R001C60, V500R005C00, V500R005C10; Secospace USG6600 versions V500R001C30, V500R001C60,	https://www.huawei.com/en/psirt/security-advisories/huawei-sa-20200715-01-outofbounds write-en	O-HUA-NGFW-190820/729

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			V500R005C00, V500R005C10; USG9500 versions V500R001C30, V500R001C60, V500R005C00, V500R005C10 **CVE ID : CVE-2020-9101**		
mate_20_rs_firmware					
Improper Limitation of a Pathname to a Restricted Directory ('Path Traversal')	17-Jul-20	2.1	HUAWEI Mate 20 versions earlier than 10.1.0.160(C00E160R3P8), HUAWEI Mate 20 X versions earlier than 10.1.0.135(C00E135R2P8), HUAWEI Mate 20 RS versions earlier than 10.1.0.160(C786E160R3P8), and Honor Magic2 smartphones versions earlier than 10.1.0.160(C00E160R2P11) have a path traversal vulnerability. The system does not sufficiently validate certain pathname from certain process, successful exploit could allow the attacker write files to a crafted path. **CVE ID : CVE-2020-9252**	https://www.huawei.com/en/psirt/security-advisories/huawei-sa-20200715-07-smartphone-en	O-HUA-MATE-190820/730
usg9500_firmware					
Out-of-bounds Write	18-Jul-20	3.3	There is an out-of-bounds write vulnerability in some products. An unauthenticated attacker crafts malformed packets with specific parameter and sends the packets to the affected products. Due	https://www.huawei.com/en/psirt/security-advisories/huawei-sa-20200715-01-	O-HUA-USG9-190820/731

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			to insufficient validation of packets, which may be exploited to cause the process reboot. Affected product versions include: IPS Module versions V500R005C00, V500R005C10; NGFW Module versions V500R005C00, V500R005C10; Secospace USG6300 versions V500R001C30, V500R001C60, V500R005C00, V500R005C10; Secospace USG6500 versions V500R001C30, V500R001C60, V500R005C00, V500R005C10; Secospace USG6600 versions V500R001C30, V500R001C60, V500R005C00, V500R005C10; USG9500 versions V500R001C30, V500R001C60, V500R005C00, V500R005C10 **CVE ID : CVE-2020-9101**	outofbounds write-en	
Juniper					
junos					
Improper Input Validation	17-Jul-20	5	An improper use of a validation framework when processing incoming genuine BGP packets within Juniper Networks RPD (routing protocols process) daemon allows an	N/A	O-JUN-JUNO-190820/732

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			attacker to crash RPD thereby causing a Denial of Service (DoS) condition. This framework requires these packets to be passed. By continuously sending any of these types of formatted genuine packets, an attacker can repeatedly crash the RPD process causing a sustained Denial of Service. Authentication to the BGP peer is not required. This issue can be initiated or propagated through eBGP and iBGP and can impact devices in either modes of use as long as the devices are configured to support the compromised framework and a BGP path is activated or active. This issue affects: Juniper Networks Junos OS 16.1 versions 16.1R7-S6 and later versions prior to 16.1R7-S8; 17.3 versions 17.3R2-S5, 17.3R3-S6 and later versions prior to 17.3R3-S8; 17.4 versions 17.4R2-S7, 17.4R3 and later versions prior to 17.4R2-S11, 17.4R3-S2; 18.1 versions 18.1R3-S7 and later versions prior to 18.1R3-S10; 18.2 versions 18.2R2-S6, 18.2R3-S2 and later versions prior to 18.2R2-S7, 18.2R3-S5;		

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			18.2X75 versions 18.2X75-D12, 18.2X75-D32, 18.2X75-D33, 18.2X75-D51, 18.2X75-D60, 18.2X75-D411, 18.2X75-D420 and later versions prior to 18.2X75-D32, 18.2X75-D33, 18.2X75-D420, 18.2X75-D52, 18.2X75-D60, 18.2X75-D65, 18.2X75-D70;(*1) 18.3 versions 18.3R1-S6, 18.3R2-S3, 18.3R3 and later versions prior to 18.3R2-S4, 18.3R3-S2; 18.4 versions 18.4R1-S5, 18.4R2-S4, 18.4R3 and later versions prior to 18.4R1-S7, 18.4R2-S5, 18.4R3-S3(*2); 19.1 versions 19.1R1-S3, 19.1R2 and later versions prior to 19.1R1-S5, 19.1R2-S2, 19.1R3-S2; 19.2 versions 19.2R1-S2, 19.2R2 and later versions prior to 19.2R1-S5, 19.2R2, 19.2R3; 19.3 versions prior to 19.3R2-S3, 19.3R3; 19.4 versions prior to 19.4R1-S2, 19.4R2, 19.4R3; 20.1 versions prior to 20.1R1-S1, 20.1R2. This issue does not affect Junos OS prior to 16.1R1. This issue affects IPv4 and IPv6 traffic. **CVE ID : CVE-2020-1640**		
Concurrent Execution using Shared	17-Jul-20	2.9	A Race Condition vulnerability in Juniper Networks Junos OS LLDP	N/A	O-JUN-JUNO-190820/733

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Resource with Improper Synchronization ('Race Condition')			implementation allows an attacker to cause LLDP to crash leading to a Denial of Service (DoS). This issue occurs when crafted LLDP packets are received by the device from an adjacent device. Multiple LACP flaps will occur after LLDP crashes. An indicator of compromise is to evaluate log file details for lldp with RLIMIT. Intervention should occur before 85% threshold of used KB versus maximum available KB memory is reached. show log messages | match RLIMIT | match lldp | last 20 Matching statement is " /kernel: %KERNEL-[number]: Process ([pid #],lldpd) has exceeded 85% of RLIMIT_DATA: " with [] as variable data to evaluate for. This issue affects: Juniper Networks Junos OS: 12.3 versions prior to 12.3R12-S15; 12.3X48 versions prior to 12.3X48-D95; 15.1 versions prior to 15.1R7-S6; 15.1X49 versions prior to 15.1X49-D200; 15.1X53 versions prior to 15.1X53-D593; 16.1 versions prior to 16.1R7-S7; 17.1 versions prior to 17.1R2-S11, 17.1R3-S2; 17.2 versions prior to 17.2R1-		

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			S9, 17.2R3-S3; 17.3 versions prior to 17.3R2-S5, 17.3R3-S6; 17.4 versions prior to 17.4R2-S4, 17.4R3; 18.1 versions prior to 18.1R3-S5; 18.2 versions prior to 18.2R2-S7, 18.2R3; 18.2X75 versions prior to 18.2X75-D12, 18.2X75-D33, 18.2X75-D50, 18.2X75-D420; 18.3 versions prior to 18.3R1-S7, 18.3R2-S3, 18.3R3; 18.4 versions prior to 18.4R1-S5, 18.4R2; 19.1 versions prior to 19.1R1-S4, 19.1R2. **CVE ID : CVE-2020-1641**		
Improper Handling of Exceptional Conditions	17-Jul-20	1.9	Execution of the "show ospf interface extensive" or "show ospf interface detail" CLI commands on a Juniper Networks device running Junos OS may cause the routing protocols process (RPD) to crash and restart if OSPF interface authentication is configured, leading to a Denial of Service (DoS). By continuously executing the same CLI commands, a local attacker can repeatedly crash the RPD process causing a sustained Denial of Service. Note: Only systems utilizing ARM processors, found on the EX2300 and EX3400, are vulnerable to this issue.	https://kb.juniper.net/JSA11030	O-JUN-JUNO-190820/734

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Systems shipped with other processor architectures are not vulnerable to this issue. The processor architecture can be displayed via the 'uname -a' command. For example: ARM (vulnerable): % uname -a | awk '{print $NF}' arm PowerPC (not vulnerable): % uname -a | awk '{print $NF}' powerpc AMD (not vulnerable): % uname -a | awk '{print $NF}' amd64 Intel (not vulnerable): % uname -a | awk '{print $NF}' i386 This issue affects Juniper Networks Junos OS: 12.3X48 versions prior to 12.3X48-D100; 14.1X53 versions prior to 14.1X53-D140, 14.1X53-D54; 15.1 versions prior to 15.1R7-S7; 15.1X49 versions prior to 15.1X49-D210; 15.1X53 versions prior to 15.1X53-D593; 16.1 versions prior to 16.1R7-S8; 17.1 versions prior to 17.1R2-S12; 17.2 versions prior to 17.2R3-S4; 17.3 versions prior to 17.3R3-S8; 17.4 versions prior to 17.4R2-S2, 17.4R3; 18.1 versions prior to 18.1R3-S2; 18.2 versions prior to 18.2R2, 18.2R3; 18.2X75 versions prior to 18.2X75-D40; 18.3 versions prior to 18.3R1-		

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			S2, 18.3R2. **CVE ID : CVE-2020-1643**		
Improper Input Validation	17-Jul-20	5	On Juniper Networks Junos OS and Junos OS Evolved devices, the receipt of a specific BGP UPDATE packet causes an internal counter to be incremented incorrectly, which over time can lead to the routing protocols process (RPD) crash and restart. This issue affects both IBGP and EBGP multihop deployment in IPv4 or IPv6 network. This issue affects: Juniper Networks Junos OS: 17.2X75 versions prior to 17.2X75-D105.19; 17.3 versions prior to 17.3R3-S8; 17.4 versions prior to 17.4R2-S10, 17.4R3-S2; 18.1 versions prior to 18.1R3-S10; 18.2 versions prior to 18.2R2-S7, 18.2R3-S4; 18.2X75 versions prior to 18.2X75-D13, 18.2X75-D411.1, 18.2X75-D420.18, 18.2X75-D52.3, 18.2X75-D60; 18.3 versions prior to 18.3R2-S4, 18.3R3-S2; 18.4 versions prior to 18.4R1-S7, 18.4R2-S4, 18.4R3-S2; 19.1 versions prior to 19.1R1-S5, 19.1R2-S1, 19.1R3; 19.2 versions prior to 19.2R1-S5, 19.2R2; 19.3 versions prior to 19.3R2-S2, 19.3R3; 19.4 versions	https://kb.juniper.net/JSA11032	O-JUN-JUNO-190820/735

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			prior to 19.4R1-S2, 19.4R2. Juniper Networks Junos OS Evolved: any releases prior to 20.1R2-EVO. This issue does not affect Juniper Networks Junos OS releases prior to 17.3R1. **CVE ID : CVE-2020-1644**		
Improper Input Validation	17-Jul-20	6.8	When DNS filtering is enabled on Juniper Networks Junos MX Series with one of the following cards MS-PIC, MS-MIC or MS-MPC, an incoming stream of packets processed by the Multiservices PIC Management Daemon (mspmand) process, responsible for managing "URL Filtering service", may crash, causing the Services PIC to restart. While the Services PIC is restarting, all PIC services including DNS filtering service (DNS sink holing) will be bypassed until the Services PIC completes its boot process. If the issue occurs, system core-dumps output will show a crash of mspmand process: root@device> show system core-dumps -rw-rw---- 1 nobody wheel 575685123 <Date> /var/tmp/pics/mspmand.core.<*>.gz This issue affects Juniper Networks Junos OS: 17.3 versions	https://kb.juniper.net/JSA11028	O-JUN-JUNO-190820/736

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			prior to 17.3R3-S8; 18.3 versions prior to 18.3R2-S4, 18.3R3-S1; 18.4 versions prior to 18.4R2-S5, 18.4R3; 19.1 versions prior to 19.1R2-S2, 19.1R3; 19.2 versions prior to 19.2R1-S5, 19.2R2; 19.3 versions prior to 19.3R2-S3, 19.3R3; 19.4 versions prior to 19.4R1-S3, 19.4R2. This issue does not affect Juniper Networks Junos OS releases prior to 17.3R2. **CVE ID : CVE-2020-1645**		
Improper Input Validation	17-Jul-20	4.3	On Juniper Networks Junos OS and Junos OS Evolved devices, processing a specific UPDATE for an EBGP peer can lead to a routing process daemon (RPD) crash and restart. This issue occurs only when the device is receiving and processing the BGP UPDATE for an EBGP peer. This issue does not occur when the device is receiving and processing the BGP UPDATE for an IBGP peer. However, the offending BGP UPDATE can originally come from an EBGP peer, propagates through the network via IBGP peers without causing crash, then it causes RPD crash when it is processed for a BGP UPDATE towards an EBGP	https://kb.juniper.net/JSA11033	O-JUN-JUNO-190820/737

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			peer. Repeated receipt and processing of the same specific BGP UPDATE can result in an extended Denial of Service (DoS) condition. This issue affects: Juniper Networks Junos OS: 17.3R3-S6, 17.4R2-S7, and 18.1R3-S7. Juniper Networks Junos OS Evolved 19.2R2-EVO and later versions, prior to 19.3R1-EVO. Other Junos OS releases are not affected. **CVE ID : CVE-2020-1646**		
Double Free	17-Jul-20	6.8	On Juniper Networks SRX Series with ICAP (Internet Content Adaptation Protocol) redirect service enabled, a double free vulnerability can lead to a Denial of Service (DoS) or Remote Code Execution (RCE) due to processing of a specific HTTP message. Continued processing of this specific HTTP message may result in an extended Denial of Service (DoS). The offending HTTP message that causes this issue may originate both from the HTTP server or the client. This issue affects Juniper Networks Junos OS on SRX Series: 18.1 versions prior to 18.1R3-S9; 18.2 versions prior to 18.2R3-S3; 18.3 versions prior to 18.3R2-	https://kb.juniper.net/JSA11034	O-JUN-JUNO-190820/738

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			S4, 18.3R3-S1; 18.4 versions prior to 18.4R2-S5, 18.4R3; 19.1 versions prior to 19.1R2; 19.2 versions prior to 19.2R1-S2, 19.2R2; 19.3 versions prior to 19.3R2. This issue does not affect Juniper Networks Junos OS prior to 18.1R1. **CVE ID : CVE-2020-1647**		
Improper Input Validation	17-Jul-20	5	On Juniper Networks Junos OS and Junos OS Evolved devices, processing a specific BGP packet can lead to a routing process daemon (RPD) crash and restart. This issue can occur even before the BGP session with the peer is established. Repeated receipt of this specific BGP packet can result in an extended Denial of Service (DoS) condition. This issue affects: Juniper Networks Junos OS: 18.2X75 versions starting from 18.2X75-D50.8, 18.2X75-D60 and later versions, prior to 18.2X75-D52.8, 18.2X75-D53, 18.2X75-D60.2, 18.2X75-D65.1, 18.2X75-D70; 19.4 versions 19.4R1 and 19.4R1-S1; 20.1 versions prior to 20.1R1-S2, 20.1R2. Juniper Networks Junos OS Evolved: 19.4-EVO versions prior to 19.4R2-S2-EVO; 20.1-EVO versions	https://kb.juniper.net/JSA11035	O-JUN-JUNO-190820/739

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			prior to 20.1R2-EVO. This issue does not affect: Juniper Networks Junos OS releases prior to 19.4R1. Juniper Networks Junos OS Evolved releases prior to 19.4R1-EVO. **CVE ID : CVE-2020-1648**		
Improper Input Validation	17-Jul-20	5	When a device running Juniper Networks Junos OS with MPC7, MPC8, or MPC9 line cards installed and the system is configured for inline IP reassembly, used by L2TP, MAP-E, GRE, and IPIP, the packet forwarding engine (PFE) will become disabled upon receipt of small fragments requiring reassembly, generating the following error messages: [LOG: Err] MQSS(2): WO: Packet Error - Error Packets 1, Connection 29 [LOG: Err] eachip_hmcif_rx_intr_handler(7259): EA[2:0]: HMCIF Rx: Injected checksum error detected on WO response - Chunk Address 0x0 [LOG: Err] MQSS(2): DRD: RORD1: CMD reorder ID error - Command 11, Reorder ID 1960, QID 0 [LOG: Err] MQSS(2): DRD: UNROLL0: HMC chunk address error in stage 5 - Chunk Address: 0xc38fb1 [LOG: Notice] Error: /fpc/0/pfe/0/cm/0/MQSS	https://kb.juniper.net/JSA11036	O-JUN-JUNO-190820/740

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			(2)/2/MQSS_CMERROR_DRD_RORD_ENG_INT_REG_CMD_FSM_STATE_ERR (0x2203cc), scope: pfe, category: functional, severity: major, module: MQSS(2), type: DRD_RORD_ENG_INT: CMD FSM State Error [LOG: Notice] Performing action cmalarm for error /fpc/0/pfe/0/cm/0/MQSS(2)/2/MQSS_CMERROR_DRD_RORD_ENG_INT_REG_CMD_FSM_STATE_ERR (0x2203cc) in module: MQSS(2) with scope: pfe category: functional level: major [LOG: Notice] Performing action get-state for error /fpc/0/pfe/0/cm/0/MQSS(2)/2/MQSS_CMERROR_DRD_RORD_ENG_INT_REG_CMD_FSM_STATE_ERR (0x2203cc) in module: MQSS(2) with scope: pfe category: functional level: major [LOG: Notice] Performing action disable-pfe for error /fpc/0/pfe/0/cm/0/MQSS(2)/2/MQSS_CMERROR_DRD_RORD_ENG_INT_REG_CMD_FSM_STATE_ERR (0x2203cc) in module: MQSS(2) with scope: pfe category: functional level: major By continuously sending fragmented packets that cannot be		

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			reassembled, an attacker can repeatedly disable the PFE causing a sustained Denial of Service (DoS). This issue affects Juniper Networks Junos OS: 17.2 versions prior to 17.2R3-S4 on MX Series; 17.3 versions prior to 17.3R3-S8 on MX Series; 17.4 versions prior to 17.4R2-S9, 17.4R3-S1 on MX Series; 18.1 versions prior to 18.1R3-S10 on MX Series; 18.2 versions prior to 18.2R2-S6, 18.2R3-S3 on MX Series; 18.2X75 versions prior to 18.2X75-D34, 18.2X75-D41, 18.2X75-D53, 18.2X75-D65, 18.2X75-D430 on MX Series; 18.3 versions prior to 18.3R1-S7, 18.3R2-S4, 18.3R3-S2 on MX Series; 18.4 versions prior to 18.4R1-S6, 18.4R2-S4, 18.4R3 on MX Series; 19.1 versions prior to 19.1R1-S4, 19.1R2-S1, 19.1R3 on MX Series; 19.2 versions prior to 19.2R1-S3, 19.2R2 on MX Series; 19.3 versions prior to 19.3R2-S2, 19.3R3 on MX Series. This issue is specific to inline IP reassembly, introduced in Junos OS 17.2. Versions of Junos OS prior to 17.2 are unaffected by this vulnerability.		

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2020-1649		
Uncontrolled Resource Consumption	17-Jul-20	5	On Juniper Networks Junos MX Series with service card configured, receipt of a stream of specific packets may crash the MS-PIC component on MS-MIC or MS-MPC. By continuously sending these specific packets, an attacker can repeatedly bring down MS-PIC on MS-MIC/MS-MPC causing a prolonged Denial of Service. This issue affects MX Series devices using MS-PIC, MS-MIC or MS-MPC service cards with any service configured. This issue affects Juniper Networks Junos OS on MX Series: 17.2R2-S7; 17.3R3-S4, 17.3R3-S5; 17.4R2-S4 and the subsequent SRs (17.4R2-S5, 17.4R2-S6, etc.); 17.4R3; 18.1R3-S3, 18.1R3-S4, 18.1R3-S5, 18.1R3-S6, 18.1R3-S7, 18.1R3-S8; 18.2R3, 18.2R3-S1, 18.2R3-S2; 18.3R2 and the SRs based on 18.3R2; 18.4R2 and the SRs based on 18.4R2; 19.1R1 and the SRs based on 19.1R1; 19.2R1 and the SRs based on 19.2R1; 19.3R1 and the SRs based on 19.3R1. **CVE ID : CVE-2020-1650**	https://kb.juniper.net/JSA11037	O-JUN-JUNO-190820/741
Missing	17-Jul-20	3.3	On Juniper Networks MX	https://kb.ju	O-JUN-JUNO-

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Release of Resource after Effective Lifetime			series, receipt of a stream of specific Layer 2 frames may cause a memory leak resulting in the packet forwarding engine (PFE) on the line card to crash and restart, causing traffic interruption. By continuously sending this stream of specific layer 2 frame, an attacker connected to the same broadcast domain can repeatedly crash the PFE, causing a prolonged Denial of Service (DoS). This issue affects Juniper Networks Junos OS on MX Series: 17.2 versions prior to 17.2R3-S4; 17.2X75 versions prior to 17.2X75-D105.19; 17.3 versions prior to 17.3R3-S7; 17.4 versions prior to 17.4R1-S3, 17.4R2; 18.1 versions prior to 18.1R2. This issue does not affect Juniper Networks Junos OS releases prior to 17.2R1. **CVE ID : CVE-2020-1651**	niper.net/JSA11038	190820/742
Improper Restriction of Operations within the Bounds of a Memory Buffer	17-Jul-20	5	On Juniper Networks Junos OS devices, a stream of TCP packets sent to the Routing Engine (RE) may cause mbuf leak which can lead to Flexible PIC Concentrator (FPC) crash or the system to crash and restart (vmcore). This issue can be trigged by IPv4 or IPv6 and it is	https://kb.juniper.net/JSA11040	O-JUN-JUNO-190820/743

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			caused only by TCP packets. This issue is not related to any specific configuration and it affects Junos OS releases starting from 17.4R1. However, this issue does not affect Junos OS releases prior to 18.2R1 when Nonstop active routing (NSR) is configured [edit routing-options nonstop-routing]. The number of mbufs is platform dependent. The following command provides the number of mbufs counter that are currently in use and maximum number of mbufs that can be allocated on a platform: user@host> show system buffers 2437/3143/5580 mbufs in use (current/cache/total) Once the device runs out of mbufs, the FPC crashes or the vmcore occurs and the device might become inaccessible requiring a manual restart. This issue affects Juniper Networks Junos OS 17.4 versions prior to 17.4R2-S11, 17.4R3-S2; 18.1 versions prior to 18.1R3-S10; 18.2 versions prior to 18.2R2-S7, 18.2R3-S5; 18.2X75 versions prior to 18.2X75-D41, 18.2X75-D420.12, 18.2X75-D51, 18.2X75-		

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			D60, 18.2X75-D34; 18.3 versions prior to 18.3R2-S4, 18.3R3-S2; 18.4 versions prior to 18.4R1-S7, 18.4R2-S4, 18.4R3-S1; 19.1 versions prior to 19.1R1-S5, 19.1R2-S1, 19.1R3; 19.2 versions prior to 19.2R1-S5, 19.2R2; 19.3 versions prior to 19.3R2-S3, 19.3R3; 19.4 versions prior to 19.4R1-S2, 19.4R2. Versions of Junos OS prior to 17.4R1 are unaffected by this vulnerability. **CVE ID : CVE-2020-1653**		
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	17-Jul-20	7.5	On Juniper Networks SRX Series with ICAP (Internet Content Adaptation Protocol) redirect service enabled, processing a malformed HTTP message can lead to a Denial of Service (DoS) or Remote Code Execution (RCE) Continued processing of this malformed HTTP message may result in an extended Denial of Service (DoS) condition. The offending HTTP message that causes this issue may originate both from the HTTP server or the HTTP client. This issue affects Juniper Networks Junos OS on SRX Series: 18.1 versions prior to 18.1R3-S9 ; 18.2 versions prior to 18.2R2-S7, 18.2R3-S3;	https://kb.juniper.net/JSA11031	O-JUN-JUNO-190820/744

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			18.3 versions prior to 18.3R1-S7, 18.3R2-S4, 18.3R3-S1; 18.4 versions prior to 18.4R1-S7, 18.4R2-S4, 18.4R3; 19.1 versions prior to 19.1R1-S5, 19.1R2; 19.2 versions prior to 19.2R1-S2, 19.2R2; 19.3 versions prior to 19.3R2. This issue does not affect Juniper Networks Junos OS prior to 18.1R1. **CVE ID : CVE-2020-1654**		
Uncontrolled Resource Consumption	17-Jul-20	5	When a device running Juniper Networks Junos OS with MPC7, MPC8, or MPC9 line cards installed and the system is configured for inline IP reassembly, used by L2TP, MAP-E, GRE, and IPIP, the packet forwarding engine (PFE) will become disabled upon receipt of large packets requiring fragmentation, generating the following error messages: [LOG: Err] MQSS(0): WO: Packet Error - Error Packets 1, Connection 29 [LOG: Err] eachip_hmcif_rx_intr_handler(7259): EA[0:0]: HMCIF Rx: Injected checksum error detected on WO response - Chunk Address 0x0 [LOG: Err] MQSS(0): DRD: RORD1: CMD reorder ID error - Command 11, Reorder ID 1838, QID 0	https://kb.juniper.net/JSA11041	O-JUN-JUNO-190820/745

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			[LOG: Err] MQSS(0): DRD: UNROLL0: HMC chunk length error in stage 5 - Chunk Address: 0x4321f3 [LOG: Err] MQSS(0): DRD: UNROLL0: HMC chunk address error in stage 5 - Chunk Address: 0x0 [LOG: Notice] Error: /fpc/8/pfe/0/cm/0/MQSS(0)/0/MQSS_CMERROR_DRD_RORD_ENG_INT_REG_CMD_FSM_STATE_ERR (0x2203cc), scope: pfe, category: functional, severity: major, module: MQSS(0), type: DRD_RORD_ENG_INT: CMD FSM State Error [LOG: Notice] Performing action cmalarm for error /fpc/8/pfe/0/cm/0/MQSS(0)/0/MQSS_CMERROR_DRD_RORD_ENG_INT_REG_CMD_FSM_STATE_ERR (0x2203cc) in module: MQSS(0) with scope: pfe category: functional level: major [LOG: Notice] Performing action get-state for error /fpc/8/pfe/0/cm/0/MQSS(0)/0/MQSS_CMERROR_DRD_RORD_ENG_INT_REG_CMD_FSM_STATE_ERR (0x2203cc) in module: MQSS(0) with scope: pfe category: functional level: major [LOG: Notice] Performing action disable-pfe for error		

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			/fpc/8/pfe/0/cm/0/MQSS(0)/0/MQSS_CMERROR_DRD_RORD_ENG_INT_REG_CMD_FSM_STATE_ERR (0x2203cc) in module: MQSS(0) with scope: pfe category: functional level: major By continuously sending fragmented packets that cannot be reassembled, an attacker can repeatedly disable the PFE causing a sustained Denial of Service (DoS). This issue affects Juniper Networks Junos OS: 17.2 versions prior to 17.2R3-S4 on MX Series; 17.3 versions prior to 17.3R3-S8 on MX Series; 17.4 versions prior to 17.4R2-S10, 17.4R3-S2 on MX Series; 18.1 versions prior to 18.1R3-S10 on MX Series; 18.2 versions prior to 18.2R3-S3 on MX Series; 18.2X75 versions prior to 18.2X75-D41, 18.2X75-D430, 18.2X75-D65 on MX Series; 18.3 versions prior to 18.3R1-S7, 18.3R2-S4, 18.3R3-S1 on MX Series; 18.4 versions prior to 18.4R1-S7, 18.4R2-S4, 18.4R3 on MX Series; 19.1 versions prior to 19.1R1-S5, 19.1R2-S1, 19.1R3 on MX Series; 19.2 versions prior to 19.2R1-S4, 19.2R2 on MX Series; 19.3 versions prior to 19.3R2-		

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			S2, 19.3R3 on MX Series. This issue is specific to inline IP reassembly, introduced in Junos OS 17.2. Versions of Junos OS prior to 17.2 are unaffected by this vulnerability. **CVE ID : CVE-2020-1655**		
junos_os_evolved					
Improper Input Validation	17-Jul-20	5	On Juniper Networks Junos OS and Junos OS Evolved devices, the receipt of a specific BGP UPDATE packet causes an internal counter to be incremented incorrectly, which over time can lead to the routing protocols process (RPD) crash and restart. This issue affects both IBGP and EBGP multihop deployment in IPv4 or IPv6 network. This issue affects: Juniper Networks Junos OS: 17.2X75 versions prior to 17.2X75-D105.19; 17.3 versions prior to 17.3R3-S8; 17.4 versions prior to 17.4R2-S10, 17.4R3-S2; 18.1 versions prior to 18.1R3-S10; 18.2 versions prior to 18.2R2-S7, 18.2R3-S4; 18.2X75 versions prior to 18.2X75-D13, 18.2X75-D411.1, 18.2X75-D420.18, 18.2X75-D52.3, 18.2X75-D60; 18.3 versions prior to 18.3R2-S4, 18.3R3-S2;	https://kb.juniper.net/JSA11032	O-JUN-JUNO-190820/746

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			18.4 versions prior to 18.4R1-S7, 18.4R2-S4, 18.4R3-S2; 19.1 versions prior to 19.1R1-S5, 19.1R2-S1, 19.1R3; 19.2 versions prior to 19.2R1-S5, 19.2R2; 19.3 versions prior to 19.3R2-S2, 19.3R3; 19.4 versions prior to 19.4R1-S2, 19.4R2. Juniper Networks Junos OS Evolved: any releases prior to 20.1R2-EVO. This issue does not affect Juniper Networks Junos OS releases prior to 17.3R1. **CVE ID : CVE-2020-1644**		
junos_evolved					
Improper Input Validation	17-Jul-20	4.3	On Juniper Networks Junos OS and Junos OS Evolved devices, processing a specific UPDATE for an EBGP peer can lead to a routing process daemon (RPD) crash and restart. This issue occurs only when the device is receiving and processing the BGP UPDATE for an EBGP peer. This issue does not occur when the device is receiving and processing the BGP UPDATE for an IBGP peer. However, the offending BGP UPDATE can originally come from an EBGP peer, propagates through the network via IBGP peers without causing crash, then it	https://kb.juniper.net/JSA11033	O-JUN-JUNO-190820/747

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			causes RPD crash when it is processed for a BGP UPDATE towards an EBGP peer. Repeated receipt and processing of the same specific BGP UPDATE can result in an extended Denial of Service (DoS) condition. This issue affects: Juniper Networks Junos OS: 17.3R3-S6, 17.4R2-S7, and 18.1R3-S7. Juniper Networks Junos OS Evolved 19.2R2-EVO and later versions, prior to 19.3R1-EVO. Other Junos OS releases are not affected. **CVE ID : CVE-2020-1646**		
Improper Input Validation	17-Jul-20	5	On Juniper Networks Junos OS and Junos OS Evolved devices, processing a specific BGP packet can lead to a routing process daemon (RPD) crash and restart. This issue can occur even before the BGP session with the peer is established. Repeated receipt of this specific BGP packet can result in an extended Denial of Service (DoS) condition. This issue affects: Juniper Networks Junos OS: 18.2X75 versions starting from 18.2X75-D50.8, 18.2X75-D60 and later versions, prior to 18.2X75-D52.8, 18.2X75-D53, 18.2X75-D60.2, 18.2X75-D65.1,	https://kb.juniper.net/JSA11035	O-JUN-JUNO-190820/748

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			18.2X75-D70; 19.4 versions 19.4R1 and 19.4R1-S1; 20.1 versions prior to 20.1R1-S2, 20.1R2. Juniper Networks Junos OS Evolved: 19.4-EVO versions prior to 19.4R2-S2-EVO; 20.1-EVO versions prior to 20.1R2-EVO. This issue does not affect: Juniper Networks Junos OS releases prior to 19.4R1. Juniper Networks Junos OS Evolved releases prior to 19.4R1-EVO. **CVE ID : CVE-2020-1648**		
Linux					
linux_kernel					
Incorrect Default Permissions	20-Jul-20	4.6	An issue was discovered in the Linux kernel 5.5 through 5.7.9, as used in Xen through 4.13.x for x86 PV guests. An attacker may be granted the I/O port permissions of an unrelated task. This occurs because tss_invalidate_io_bitmap mishandling causes a loss of synchronization between the I/O bitmaps of TSS and Xen, aka CID-cadfad870154. **CVE ID : CVE-2020-15852**	https://security.netapp.com/advisory/ntap-20200810-0001/	O-LIN-LINU-190820/749
Information Exposure	30-Jul-20	4.3	The Linux kernel through 5.7.11 allows remote attackers to make observations that help to obtain sensitive	https://security.netapp.com/advisory/ntap-20200814-	O-LIN-LINU-190820/750

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			information about the internal state of the network RNG, aka CID-f227e3ec3b5c. This is related to drivers/char/random.c and kernel/time/timer.c. **CVE ID : CVE-2020-16166**	0004/	
Microsoft					
windows					
Unquoted Search Path or Element	29-Jul-20	6.8	TeamViewer Desktop for Windows before 15.8.3 does not properly quote its custom URI handlers. A malicious website could launch TeamViewer with arbitrary parameters, as demonstrated by a teamviewer10: --play URL. An attacker could force a victim to send an NTLM authentication request and either relay the request or capture the hash for offline password cracking. This affects teamviewer10, teamviewer8, teamviewerapi, tvchat1, tvcontrol1, tvfiletransfer1, tvjoinv8, tvpresent1, tvsendfile1, tvsqcustomer1, tvsqsupport1, tvvideocall1, and tvvpn1. The issue is fixed in 8.0.258861, 9.0.258860, 10.0.258873, 11.0.258870, 12.0.258869, 13.2.36220, 14.2.56676, 14.7.48350, and 15.8.3.	https://community.teamviewer.com/t5/Announcements/Statement-on-CVE-2020-13699/td-p/98448	O-MIC-WIND-190820/751

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2020-13699		
Improper Limitation of a Pathname to a Restricted Directory ('Path Traversal')	27-Jul-20	5	SteelCentral Aternity Agent before 11.0.0.120 on Windows allows Privilege Escalation via a crafted file. It uses an executable running as a high privileged Windows service to perform administrative tasks and collect data from other processes. It distributes functionality among different processes and uses IPC (Inter-Process Communication) primitives to enable the processes to cooperate. The remotely callable methods from remotable objects available through interprocess communication allow loading of arbitrary plugins (i.e., C# assemblies) from the "%PROGRAMFILES(X86)%/Aternity Information Systems/Assistant/plugins" directory, where the name of the plugin is passed as part of an XML-serialized object. However, because the name of the DLL is concatenated with the ".\plugins" string, a directory traversal vulnerability exists in the way plugins are resolved. **CVE ID : CVE-2020-15592**	https://aternity.force.com/customersuccess/s/article/Recorder-tool-security-notification-mitigation-steps-for-On-Prem	O-MIC-WIND-190820/752

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Incorrect Permission Assignment for Critical Resource	27-Jul-20	7.2	SteelCentral Aternity Agent 11.0.0.120 on Windows mishandles IPC. It uses an executable running as a high privileged Windows service to perform administrative tasks and collect data from other processes. It distributes functionality among different processes and uses IPC (Inter-Process Communication) primitives to enable the processes to cooperate. Any user in the system is allowed to access the interprocess communication channel AternityAgentAssistantIpc, retrieve a serialized object and call object methods remotely. Among others, the methods allow any user to: (1) Create and/or overwrite arbitrary XML files across the system; (2) Create arbitrary directories across the system; and (3) Load arbitrary plugins (i.e., C# assemblies) from the "%PROGRAMFILES(X86)/ Aternity Information Systems/Assistant/plugins ” directory and execute code contained in them. **CVE ID : CVE-2020-15593**	https://aternity.force.com/customersuccess/s/article/Recorder-tool-security-notification-mitigation-steps-for-On-Prem	O-MIC-WIND-190820/753
Use After	30-Jul-20	6.8	DaviewIndy 8.98.7 and earlier version contain	N/A	O-MIC-WIND-

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Free			Use-After-Free vulnerability, triggered when the user opens a malformed specific file that is mishandled by Daview.exe. Attackers could exploit this and arbitrary code execution. **CVE ID : CVE-2020-7827**		190820/754
Out-of-bounds Write	30-Jul-20	6.8	DaviewIndy 8.98.4 and earlier version contain Heap-based overflow vulnerability, triggered when the user opens a malformed specific file that is mishandled by Daview.exe. Attackers could exploit this and arbitrary code execution. **CVE ID : CVE-2020-7828**	N/A	O-MIC-WIND-190820/755
Out-of-bounds Write	30-Jul-20	6.8	DaviewIndy 8.98.4 and earlier version contain Heap-based overflow vulnerability, triggered when the user opens a malformed specific file that is mishandled by Daview.exe. Attackers could exploit this and arbitrary code execution. **CVE ID : CVE-2020-7829**	N/A	O-MIC-WIND-190820/756
Improper Privilege Management	17-Jul-20	7.5	Adobe Creative Cloud Desktop Application versions 5.1 and earlier have a lack of exploit mitigations vulnerability. Successful exploitation could lead to privilege escalation.	https://helpx.adobe.com/security/products/creative-cloud/apsb20-33.html	O-MIC-WIND-190820/757

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2020-9669		
Improper Link Resolution Before File Access ('Link Following')	17-Jul-20	7.5	Adobe Creative Cloud Desktop Application versions 5.1 and earlier have a symlink vulnerability vulnerability. Successful exploitation could lead to privilege escalation. **CVE ID : CVE-2020-9670**	https://helpx.adobe.com/security/products/creative-cloud/apsb20-33.html	O-MIC-WIND-190820/758
Improper Privilege Management	17-Jul-20	7.5	Adobe Creative Cloud Desktop Application versions 5.1 and earlier have an insecure file permissions vulnerability. Successful exploitation could lead to privilege escalation. **CVE ID : CVE-2020-9671**	https://helpx.adobe.com/security/products/creative-cloud/apsb20-33.html	O-MIC-WIND-190820/759
Out-of-bounds Write	22-Jul-20	6.8	Adobe Bridge versions 10.0.3 and earlier have an out-of-bounds write vulnerability. Successful exploitation could lead to arbitrary code execution. **CVE ID : CVE-2020-9674**	https://helpx.adobe.com/security/products/bridge/apsb20-44.html	O-MIC-WIND-190820/760
Out-of-bounds Read	22-Jul-20	6.8	Adobe Bridge versions 10.0.3 and earlier have an out-of-bounds read vulnerability. Successful exploitation could lead to arbitrary code execution. **CVE ID : CVE-2020-9675**	https://helpx.adobe.com/security/products/bridge/apsb20-44.html	O-MIC-WIND-190820/761
Out-of-bounds Write	22-Jul-20	6.8	Adobe Bridge versions 10.0.3 and earlier have an out-of-bounds write vulnerability. Successful exploitation could lead to	https://helpx.adobe.com/security/products/bridge/apsb20-	O-MIC-WIND-190820/762

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			arbitrary code execution. **CVE ID : CVE-2020-9676**	44.html	
Out-of-bounds Write	22-Jul-20	6.8	Adobe Prelude versions 9.0 and earlier have an out-of-bounds read vulnerability. Successful exploitation could lead to arbitrary code execution. **CVE ID : CVE-2020-9677**	https://helpx.adobe.com/security/products/prelude/apsb20-46.html	O-MIC-WIND-190820/763
Out-of-bounds Write	22-Jul-20	6.8	Adobe Prelude versions 9.0 and earlier have an out-of-bounds write vulnerability. Successful exploitation could lead to arbitrary code execution . **CVE ID : CVE-2020-9678**	https://helpx.adobe.com/security/products/prelude/apsb20-46.html	O-MIC-WIND-190820/764
Out-of-bounds Read	22-Jul-20	4.3	Adobe Prelude versions 9.0 and earlier have an out-of-bounds read vulnerability. Successful exploitation could lead to arbitrary code execution. **CVE ID : CVE-2020-9679**	https://helpx.adobe.com/security/products/prelude/apsb20-46.html	O-MIC-WIND-190820/765
Out-of-bounds Write	22-Jul-20	6.8	Adobe Prelude versions 9.0 and earlier have an out-of-bounds write vulnerability. Successful exploitation could lead to arbitrary code execution . **CVE ID : CVE-2020-9680**	https://helpx.adobe.com/security/products/prelude/apsb20-46.html	O-MIC-WIND-190820/766
Improper Link Resolution Before File Access ('Link Following')	17-Jul-20	10	Adobe Creative Cloud Desktop Application versions 5.1 and earlier have a symlink vulnerability vulnerability. Successful exploitation could lead to arbitrary file system write.	https://helpx.adobe.com/security/products/creative-cloud/apsb20-33.html	O-MIC-WIND-190820/767

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2020-9682		
Out-of-bounds Write	22-Jul-20	6.8	Adobe Photoshop versions Photoshop CC 2019, and Photoshop 2020 have an out-of-bounds read vulnerability. Successful exploitation could lead to arbitrary code execution. **CVE ID : CVE-2020-9683**	https://helpx.adobe.com/security/products/photoshop/apsb20-45.html	O-MIC-WIND-190820/768
Out-of-bounds Write	22-Jul-20	6.8	Adobe Photoshop versions Photoshop CC 2019, and Photoshop 2020 have an out-of-bounds write vulnerability. Successful exploitation could lead to arbitrary code execution . **CVE ID : CVE-2020-9684**	https://helpx.adobe.com/security/products/photoshop/apsb20-45.html	O-MIC-WIND-190820/769
Out-of-bounds Write	22-Jul-20	6.8	Adobe Photoshop versions Photoshop CC 2019, and Photoshop 2020 have an out-of-bounds write vulnerability. Successful exploitation could lead to arbitrary code execution . **CVE ID : CVE-2020-9685**	https://helpx.adobe.com/security/products/photoshop/apsb20-45.html	O-MIC-WIND-190820/770
Out-of-bounds Read	22-Jul-20	4.3	Adobe Photoshop versions Photoshop CC 2019, and Photoshop 2020 have an out-of-bounds read vulnerability. Successful exploitation could lead to arbitrary code execution. **CVE ID : CVE-2020-9686**	https://helpx.adobe.com/security/products/photoshop/apsb20-45.html	O-MIC-WIND-190820/771
Out-of-bounds Write	22-Jul-20	6.8	Adobe Photoshop versions Photoshop CC 2019, and Photoshop 2020 have an out-of-bounds write vulnerability. Successful	https://helpx.adobe.com/security/products/photoshop/apsb2	O-MIC-WIND-190820/772

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			exploitation could lead to arbitrary code execution . **CVE ID : CVE-2020-9687**	0-45.html	
Improper Neutralization of Special Elements in Output Used by a Downstream Component ('Injection')	17-Jul-20	9.3	Adobe Download Manager version 2.0.0.518 have a command injection vulnerability. Successful exploitation could lead to arbitrary code execution. **CVE ID : CVE-2020-9688**	https://helpx.adobe.com/security/products/adm/apsb20-49.html	O-MIC-WIND-190820/773
windows_10					
Improper Restriction of Operations within the Bounds of a Memory Buffer	27-Jul-20	6.8	A remote code execution vulnerability exists in the way that Microsoft Windows Codecs Library handles objects in memory, aka 'Microsoft Windows Codecs Library Remote Code Execution Vulnerability'. This CVE ID is unique from CVE-2020-1425. **CVE ID : CVE-2020-1457**	N/A	O-MIC-WIND-190820/774
Improper Restriction of Operations within the Bounds of a Memory Buffer	27-Jul-20	6.8	A remoted code execution vulnerability exists in the way that Microsoft Windows Codecs Library handles objects in memory, aka 'Microsoft Windows Codecs Library Remote Code Execution Vulnerability'. This CVE ID is unique from CVE-2020-1457. **CVE ID : CVE-2020-1425**	N/A	O-MIC-WIND-190820/775
Improper Verification	29-Jul-20	4.4	GRUB2 fails to validate kernel signature when	https://lists.gnu.org/arch	O-MIC-WIND-

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
of Cryptographic Signature			booted directly without shim, allowing secure boot to be bypassed. This only affects systems where the kernel signing certificate has been imported directly into the secure boot database and the GRUB image is booted directly without the use of shim. This issue affects GRUB2 version 2.04 and prior versions. **CVE ID : CVE-2020-15705**	ive/html/grub-devel/2020-07/msg00034.html, https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/ADV200011, https://security.netapp.com/advisory/ntap-20200731-0008/	190820/776
Concurrent Execution using Shared Resource with Improper Synchronization ('Race Condition')	29-Jul-20	4.4	GRUB2 contains a race condition in grub_script_function_create() leading to a use-after-free vulnerability which can be triggered by redefining a function whilst the same function is already executing, leading to arbitrary code execution and secure boot restriction bypass. This issue affects GRUB2 version 2.04 and prior versions. **CVE ID : CVE-2020-15706**	https://lists.gnu.org/archive/html/grub-devel/2020-07/msg00034.html, https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/ADV200011, https://security.netapp.com/advisory/ntap-20200731-0008/	O-MIC-WIND-190820/777
Concurrent Execution using Shared	29-Jul-20	4.4	Integer overflows were discovered in the functions grub_cmd_initrd and	https://lists.gnu.org/archive/html/gru	O-MIC-WIND-190820/778

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Resource with Improper Synchronization ('Race Condition')			grub_initrd_init in the efilinux component of GRUB2, as shipped in Debian, Red Hat, and Ubuntu (the functionality is not included in GRUB2 upstream), leading to a heap-based buffer overflow. These could be triggered by an extremely large number of arguments to the initrd command on 32-bit architectures, or a crafted filesystem with very large files on any architecture. An attacker could use this to execute arbitrary code and bypass UEFI Secure Boot restrictions. This issue affects GRUB2 version 2.04 and prior versions. **CVE ID : CVE-2020-15707**	b-devel/2020-07/msg00034.html, https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/ADV200011, https://security.netapp.com/advisory/ntap-20200731-0008/	
windows_8.1					
Improper Verification of Cryptographic Signature	29-Jul-20	4.4	GRUB2 fails to validate kernel signature when booted directly without shim, allowing secure boot to be bypassed. This only affects systems where the kernel signing certificate has been imported directly into the secure boot database and the GRUB image is booted directly without the use of shim. This issue affects GRUB2 version 2.04 and prior versions.	https://lists.gnu.org/archive/html/grub-devel/2020-07/msg00034.html, https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/ADV200011, https://secu	O-MIC-WIND-190820/779

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2020-15705	rity.netapp.com/advisory/ntap-20200731-0008/	
Concurrent Execution using Shared Resource with Improper Synchronization ('Race Condition')	29-Jul-20	4.4	GRUB2 contains a race condition in grub_script_function_create() leading to a use-after-free vulnerability which can be triggered by redefining a function whilst the same function is already executing, leading to arbitrary code execution and secure boot restriction bypass. This issue affects GRUB2 version 2.04 and prior versions. **CVE ID : CVE-2020-15706**	https://lists.gnu.org/archive/html/grub-devel/2020-07/msg00034.html, https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/ADV200011, https://security.netapp.com/advisory/ntap-20200731-0008/	O-MIC-WIND-190820/780
Concurrent Execution using Shared Resource with Improper Synchronization ('Race Condition')	29-Jul-20	4.4	Integer overflows were discovered in the functions grub_cmd_initrd and grub_initrd_init in the efilinux component of GRUB2, as shipped in Debian, Red Hat, and Ubuntu (the functionality is not included in GRUB2 upstream), leading to a heap-based buffer overflow. These could be triggered by an extremely large number of arguments to the initrd command on 32-bit	https://lists.gnu.org/archive/html/grub-devel/2020-07/msg00034.html, https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/ADV200011, https://security.netapp.c	O-MIC-WIND-190820/781

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			architectures, or a crafted filesystem with very large files on any architecture. An attacker could use this to execute arbitrary code and bypass UEFI Secure Boot restrictions. This issue affects GRUB2 version 2.04 and prior versions. **CVE ID : CVE-2020-15707**	om/advisory/ntap-20200731-0008/	
windows_rt_8.1					
Improper Verification of Cryptographic Signature	29-Jul-20	4.4	GRUB2 fails to validate kernel signature when booted directly without shim, allowing secure boot to be bypassed. This only affects systems where the kernel signing certificate has been imported directly into the secure boot database and the GRUB image is booted directly without the use of shim. This issue affects GRUB2 version 2.04 and prior versions. **CVE ID : CVE-2020-15705**	https://lists.gnu.org/archive/html/grub-devel/2020-07/msg00034.html, https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/ADV200011, https://security.netapp.com/advisory/ntap-20200731-0008/	O-MIC-WIND-190820/782
Concurrent Execution using Shared Resource with Improper Synchronization ('Race	29-Jul-20	4.4	GRUB2 contains a race condition in grub_script_function_create() leading to a use-after-free vulnerability which can be triggered by redefining a function whilst the same function is	https://lists.gnu.org/archive/html/grub-devel/2020-07/msg00034.html, https://port	O-MIC-WIND-190820/783

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Condition')			already executing, leading to arbitrary code execution and secure boot restriction bypass. This issue affects GRUB2 version 2.04 and prior versions. **CVE ID : CVE-2020-15706**	al.msrc.microsoft.com/en-US/security-guidance/advisory/ADV200011, https://security.netapp.com/advisory/ntap-20200731-0008/	
Concurrent Execution using Shared Resource with Improper Synchronization ('Race Condition')	29-Jul-20	4.4	Integer overflows were discovered in the functions grub_cmd_initrd and grub_initrd_init in the efilinux component of GRUB2, as shipped in Debian, Red Hat, and Ubuntu (the functionality is not included in GRUB2 upstream), leading to a heap-based buffer overflow. These could be triggered by an extremely large number of arguments to the initrd command on 32-bit architectures, or a crafted filesystem with very large files on any architecture. An attacker could use this to execute arbitrary code and bypass UEFI Secure Boot restrictions. This issue affects GRUB2 version 2.04 and prior versions. **CVE ID : CVE-2020-15707**	https://lists.gnu.org/archive/html/grub-devel/2020-07/msg00034.html, https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/ADV200011, https://security.netapp.com/advisory/ntap-20200731-0008/	O-MIC-WIND-190820/784
windows_server_2012					

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Improper Verification of Cryptographic Signature	29-Jul-20	4.4	GRUB2 fails to validate kernel signature when booted directly without shim, allowing secure boot to be bypassed. This only affects systems where the kernel signing certificate has been imported directly into the secure boot database and the GRUB image is booted directly without the use of shim. This issue affects GRUB2 version 2.04 and prior versions. **CVE ID : CVE-2020-15705**	https://lists.gnu.org/archive/html/grub-devel/2020-07/msg00034.html, https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/ADV200011, https://security.netapp.com/advisory/ntap-20200731-0008/	O-MIC-WIND-190820/785
Concurrent Execution using Shared Resource with Improper Synchronization ('Race Condition')	29-Jul-20	4.4	GRUB2 contains a race condition in grub_script_function_create() leading to a use-after-free vulnerability which can be triggered by redefining a function whilst the same function is already executing, leading to arbitrary code execution and secure boot restriction bypass. This issue affects GRUB2 version 2.04 and prior versions. **CVE ID : CVE-2020-15706**	https://lists.gnu.org/archive/html/grub-devel/2020-07/msg00034.html, https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/ADV200011, https://security.netapp.com/advisory/ntap-20200731-0008/	O-MIC-WIND-190820/786

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Concurrent Execution using Shared Resource with Improper Synchronization ('Race Condition')	29-Jul-20	4.4	Integer overflows were discovered in the functions grub_cmd_initrd and grub_initrd_init in the efilinux component of GRUB2, as shipped in Debian, Red Hat, and Ubuntu (the functionality is not included in GRUB2 upstream), leading to a heap-based buffer overflow. These could be triggered by an extremely large number of arguments to the initrd command on 32-bit architectures, or a crafted filesystem with very large files on any architecture. An attacker could use this to execute arbitrary code and bypass UEFI Secure Boot restrictions. This issue affects GRUB2 version 2.04 and prior versions. **CVE ID : CVE-2020-15707**	https://lists.gnu.org/archive/html/grub-devel/2020-07/msg00034.html, https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/ADV200011, https://security.netapp.com/advisory/ntap-20200731-0008/	O-MIC-WIND-190820/787
windows_server_2016					
Improper Verification of Cryptographic Signature	29-Jul-20	4.4	GRUB2 fails to validate kernel signature when booted directly without shim, allowing secure boot to be bypassed. This only affects systems where the kernel signing certificate has been imported directly into the secure boot database and the GRUB image is booted directly without the use of shim.	https://lists.gnu.org/archive/html/grub-devel/2020-07/msg00034.html, https://portal.msrc.microsoft.com/en-US/security-guidance/ad	O-MIC-WIND-190820/788

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			This issue affects GRUB2 version 2.04 and prior versions. **CVE ID : CVE-2020-15705**	visory/ADV200011, https://security.netapp.com/advisory/ntap-20200731-0008/	
Concurrent Execution using Shared Resource with Improper Synchronization ('Race Condition')	29-Jul-20	4.4	GRUB2 contains a race condition in grub_script_function_create() leading to a use-after-free vulnerability which can be triggered by redefining a function whilst the same function is already executing, leading to arbitrary code execution and secure boot restriction bypass. This issue affects GRUB2 version 2.04 and prior versions. **CVE ID : CVE-2020-15706**	https://lists.gnu.org/archive/html/grub-devel/2020-07/msg00034.html, https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/ADV200011, https://security.netapp.com/advisory/ntap-20200731-0008/	O-MIC-WIND-190820/789
Concurrent Execution using Shared Resource with Improper Synchronization ('Race Condition')	29-Jul-20	4.4	Integer overflows were discovered in the functions grub_cmd_initrd and grub_initrd_init in the efilinux component of GRUB2, as shipped in Debian, Red Hat, and Ubuntu (the functionality is not included in GRUB2 upstream), leading to a heap-based buffer overflow. These could be triggered by an extremely	https://lists.gnu.org/archive/html/grub-devel/2020-07/msg00034.html, https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/ADV2	O-MIC-WIND-190820/790

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			large number of arguments to the initrd command on 32-bit architectures, or a crafted filesystem with very large files on any architecture. An attacker could use this to execute arbitrary code and bypass UEFI Secure Boot restrictions. This issue affects GRUB2 version 2.04 and prior versions. **CVE ID : CVE-2020-15707**	00011, https://security.netapp.com/advisory/ntap-20200731-0008/	
windows_server_2019					
Improper Verification of Cryptographic Signature	29-Jul-20	4.4	GRUB2 fails to validate kernel signature when booted directly without shim, allowing secure boot to be bypassed. This only affects systems where the kernel signing certificate has been imported directly into the secure boot database and the GRUB image is booted directly without the use of shim. This issue affects GRUB2 version 2.04 and prior versions. **CVE ID : CVE-2020-15705**	https://lists.gnu.org/archive/html/grub-devel/2020-07/msg00034.html, https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/ADV200011, https://security.netapp.com/advisory/ntap-20200731-0008/	O-MIC-WIND-190820/791
Concurrent Execution using Shared Resource with	29-Jul-20	4.4	GRUB2 contains a race condition in grub_script_function_create() leading to a use-after-free vulnerability which	https://lists.gnu.org/archive/html/grub-devel/2020-	O-MIC-WIND-190820/792

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Improper Synchronization ('Race Condition')			can be triggered by redefining a function whilst the same function is already executing, leading to arbitrary code execution and secure boot restriction bypass. This issue affects GRUB2 version 2.04 and prior versions. **CVE ID : CVE-2020-15706**	07/msg00034.html, https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/ADV200011, https://security.netapp.com/advisory/ntap-20200731-0008/	
Concurrent Execution using Shared Resource with Improper Synchronization ('Race Condition')	29-Jul-20	4.4	Integer overflows were discovered in the functions grub_cmd_initrd and grub_initrd_init in the efilinux component of GRUB2, as shipped in Debian, Red Hat, and Ubuntu (the functionality is not included in GRUB2 upstream), leading to a heap-based buffer overflow. These could be triggered by an extremely large number of arguments to the initrd command on 32-bit architectures, or a crafted filesystem with very large files on any architecture. An attacker could use this to execute arbitrary code and bypass UEFI Secure Boot restrictions. This issue affects GRUB2 version 2.04 and prior versions.	https://lists.gnu.org/archive/html/grub-devel/2020-07/msg00034.html, https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/ADV200011, https://security.netapp.com/advisory/ntap-20200731-0008/	O-MIC-WIND-190820/793

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2020-15707		
Netgear					
r6700_firmware					
Authentication Bypass by Primary Weakness	28-Jul-20	8.3	This vulnerability allows network-adjacent attackers to bypass authentication on affected installations of NETGEAR R6700 V1.0.4.84_10.0.58 routers. Authentication is not required to exploit this vulnerability. The specific flaw exists within the UPnP service, which listens on TCP port 5000. A crafted UPnP message can be used to bypass authentication. An attacker can leverage this in conjunction with other vulnerabilities to execute arbitrary code in the context of root. Was ZDI-CAN-9642. **CVE ID : CVE-2020-10923**	N/A	O-NET-R670-190820/794
Stack-based Buffer Overflow	28-Jul-20	8.3	This vulnerability allows network-adjacent attackers to bypass authentication on affected installations of NETGEAR R6700 V1.0.4.84_10.0.58 routers. Although authentication is required to exploit this vulnerability, the existing authentication mechanism can be bypassed. The specific flaw exists within the UPnP service, which listens on TCP port 5000	N/A	O-NET-R670-190820/795

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			by default. The issue results from the lack of proper validation of the length of user-supplied data prior to copying it to a fixed-length, stack-based buffer. An attacker can leverage this vulnerability to execute code in the context of root. Was ZDI-CAN-9643. **CVE ID : CVE-2020-10924**		
Improper Certificate Validation	28-Jul-20	8.3	This vulnerability allows network-adjacent attackers to compromise the integrity of downloaded information on affected installations of NETGEAR R6700 V1.0.4.84_10.0.58 routers. Authentication is not required to exploit this vulnerability. The specific flaw exists within the downloading of files via HTTPS. The issue results from the lack of proper validation of the certificate presented by the server. An attacker can leverage this in conjunction with other vulnerabilities to execute arbitrary code in the context of root. Was ZDI-CAN-9647. **CVE ID : CVE-2020-10925**	N/A	O-NET-R670-190820/796
Download of Code Without Integrity	28-Jul-20	8.3	This vulnerability allows network-adjacent attackers to execute arbitrary code on affected	N/A	O-NET-R670-190820/797

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Check			installations of NETGEAR R6700 V1.0.4.84_10.0.58 routers. Authentication is not required to exploit this vulnerability. The specific flaw exists within the handling of firmware updates. The issue results from the lack of proper validation of the firmware image prior to performing an upgrade. An attacker can leverage this in conjunction with other vulnerabilities to execute code in the context of root. Was ZDI-CAN-9648. **CVE ID : CVE-2020-10926**		
Use of a Broken or Risky Cryptographic Algorithm	28-Jul-20	8.3	This vulnerability allows network-adjacent attackers to execute arbitrary code on affected installations of NETGEAR R6700 V1.0.4.84_10.0.58 routers. Authentication is not required to exploit this vulnerability. The specific flaw exists within the encryption of firmware update images. The issue results from the use of an inappropriate encryption algorithm. An attacker can leverage this in conjunction with other vulnerabilities to execute code in the context of root. Was ZDI-CAN-9649. **CVE ID : CVE-2020-10927**	N/A	O-NET-R670-190820/798
Heap-based	28-Jul-20	4.6	This vulnerability allows	N/A	O-NET-R670-

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Buffer Overflow			network-adjacent attackers to execute arbitrary code on affected installations of NETGEAR R6700 V1.0.4.84_10.0.58 routers. Authentication is not required to exploit this vulnerability. The specific flaw exists within the handling of string table file uploads. The issue results from the lack of proper validation of the length of user-supplied data prior to copying it to a fixed-length, heap-based buffer. An attacker can leverage this vulnerability to execute code in the context of the web server. Was ZDI-CAN-9767. **CVE ID : CVE-2020-10928**		190820/799
Integer Overflow or Wraparound	28-Jul-20	8.3	This vulnerability allows network-adjacent attackers to execute arbitrary code on affected installations of NETGEAR R6700 V1.0.4.84_10.0.58 routers. Authentication is not required to exploit this vulnerability. The specific flaw exists within the handling of string table file uploads. The issue results from the lack of proper validation of user-supplied data, which can result in an integer overflow before allocating a buffer. An attacker can leverage this vulnerability to execute	N/A	O-NET-R670-190820/800

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			code in the context of the admin user. Was ZDI-CAN-9768. **CVE ID : CVE-2020-10929**		
Improper Access Control	28-Jul-20	3.3	This vulnerability allows network-adjacent attackers to disclose sensitive information on affected installations of NETGEAR R6700 V1.0.4.84_10.0.58 routers. Authentication is not required to exploit this vulnerability. The specific flaw exists within the handling of URLs. The issue results from the lack of proper routing of URLs. An attacker can leverage this vulnerability to disclose stored credentials, leading to further compromise. Was ZDI-CAN-9618. **CVE ID : CVE-2020-10930**	N/A	O-NET-R670-190820/801
Stack-based Buffer Overflow	28-Jul-20	8.3	This vulnerability allows network-adjacent attackers to bypass authentication on affected installations of NETGEAR R6700 V1.0.4.84_10.0.58 routers. Authentication is not required to exploit this vulnerability. The specific flaw exists within the httpd service, which listens on TCP port 80 by default. The issue results from the lack of proper validation of the length of	N/A	O-NET-R670-190820/802

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			user-supplied data prior to copying it to a fixed-length, stack-based buffer. An attacker can leverage this vulnerability to execute code in the context of root. Was ZDI-CAN-9703. **CVE ID : CVE-2020-15416**		
Stack-based Buffer Overflow	28-Jul-20	5.8	This vulnerability allows network-adjacent attackers to execute arbitrary code on affected installations of NETGEAR R6700 V1.0.4.84_10.0.58 routers. Authentication is not required to exploit this vulnerability. The specific flaw exists within the handling of string table file uploads. A crafted gui_region in a string table file can trigger an overflow of a fixed-length stack-based buffer. An attacker can leverage this vulnerability to execute code in the context of the web server. Was ZDI-CAN-9756. **CVE ID : CVE-2020-15417**	N/A	O-NET-R670-190820/803
Openbsd					
openbsd					
Authorization Bypass Through User-Controlled Key	28-Jul-20	7.5	iked in OpenIKED, as used in OpenBSD through 6.7, allows authentication bypass because ca.c has the wrong logic for checking whether a public key matches.	https://ftp.openbsd.org/pub/OpenBSD/patches/6.7/common/014_iked.patch.sig	O-OPE-OPEN-190820/804

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2020-16088		
Opensuse					
leap					
Concurrent Execution using Shared Resource with Improper Synchronization ('Race Condition')	17-Jul-20	4.4	In cdev_get of char_dev.c, there is a possible use-after-free due to a race condition. This could lead to local escalation of privilege with System execution privileges needed. User interaction is not needed for exploitation.Product: AndroidVersions: Android-10Android ID: A-153467744 **CVE ID : CVE-2020-0305**	https://source.android.com/security/bulletin/pixel/2020-06-01	O-OPE-LEAP-190820/805
Information Exposure	30-Jul-20	4.3	The Linux kernel through 5.7.11 allows remote attackers to make observations that help to obtain sensitive information about the internal state of the network RNG, aka CID-f227e3ec3b5c. This is related to drivers/char/random.c and kernel/time/timer.c. **CVE ID : CVE-2020-16166**	https://security.netapp.com/advisory/ntap-20200814-0004/	O-OPE-LEAP-190820/806
Qualcomm					
qca6574au_firmware					
Buffer Copy without Checking Size of Input ('Classic Buffer	30-Jul-20	7.5	Possible buffer overflow while parsing mp4 clip with corrupted sample atoms due to improper validation of index in Snapdragon Auto,	https://www.qualcomm.com/company/product-security/bulletins/july-	O-QUA-QCA6-190820/807

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Overflow')			Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables in APQ8009, APQ8017, APQ8053, APQ8096AU, APQ8098, Kamorta, MDM9206, MDM9207C, MDM9607, MSM8905, MSM8909W, MSM8917, MSM8920, MSM8937, MSM8940, MSM8953, MSM8996, MSM8996AU, MSM8998, Nicobar, QCA6574AU, QCM2150, QCS405, QCS605, QM215, Rennell, SA6155P, Saipan, SDA660, SDA845, SDM429, SDM429W, SDM439, SDM450, SDM630, SDM632, SDM636, SDM660, SDM670, SDM710, SDM845, SDX20, SM6150, SM7150, SM8150, SM8250, SXR1130, SXR2130 **CVE ID : CVE-2020-3688**	2020-bulletin	
Out-of-bounds Write	30-Jul-20	7.5	Out of bound write while QoS DSCP mapping due to improper input validation for data received from association response frame in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial	https://www.qualcomm.com/company/product-security/bulletins/july-2020-bulletin	O-QUA-QCA6-190820/808

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables in APQ8009, APQ8017, APQ8053, APQ8096AU, APQ8098, MDM9150, MDM9206, MDM9207C, MDM9607, MDM9650, MSM8905, MSM8909W, MSM8917, MSM8920, MSM8937, MSM8940, MSM8953, MSM8996AU, Nicobar, QCA6174A, QCA6574AU, QCA9377, QCA9379, QCM2150, QCN7605, QCS405, QCS605, QM215, SA6155P, Saipan, SC8180X, SDA845, SDM429, SDM429W, SDM439, SDM450, SDM630, SDM632, SDM636, SDM660, SDM845, SDX20, SDX55, SM8150, SM8250, SXR2130 **CVE ID : CVE-2020-3698**		
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	30-Jul-20	7.5	Possible out of bound access while processing assoc response from host due to improper length check before copying into buffer 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,	https://www.qualcomm.com/company/product-security/bulletins/july-2020-bulletin	O-QUA-QCA6-190820/809

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			APQ8053, APQ8096AU, MDM9206, MDM9207C, MDM9607, MDM9640, MDM9650, MSM8905, MSM8909W, MSM8917, MSM8920, MSM8937, MSM8940, MSM8953, MSM8996AU, Nicobar, QCA6174A, QCA6574AU, QCA9377, QCA9379, QCM2150, QCN7605, QCS405, QCS605, QM215, SA6155P, Saipan, SC8180X, SDA845, SDM429, SDM429W, SDM439, SDM450, SDM630, SDM632, SDM636, SDM660, SDM845, SDX20, SDX55, SM6150, SM7150, SM8150, SM8250, SXR2130 **CVE ID : CVE-2020-3699**		
Out-of-bounds Read	30-Jul-20	5	Possible out of bounds read due to a missing bounds check and could lead to local information disclosure in the wifi driver with no additional execution privileges needed in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking in APQ8053,	https://www.qualcomm.com/company/product-security/bulletins/july-2020-bulletin	O-QUA-QCA6-190820/810

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			APQ8096AU, IPQ4019, IPQ8064, IPQ8074, MDM9607, MSM8909W, MSM8996AU, QCA6574AU, QCA9531, QCA9558, QCA9980, SC8180X, SDM439, SDX55, SM8150, SM8250, SXR2130 **CVE ID : CVE-2020-3700**		
qcs405_firmware					
Use After Free	30-Jul-20	7.5	Use-after-free issue could occur due to dangling pointer when generating a frame buffer in OpenGL ES in Snapdragon Compute, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music in APQ8009, Nicobar, QCM2150, QCS405, Saipan, SDM845, SM8150, SM8250, SXR2130 **CVE ID : CVE-2020-3671**	https://www.qualcomm.com/company/product-security/bulletins/july-2020-bulletin	O-QUA-QCS4-190820/811
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	30-Jul-20	7.5	Possible buffer overflow while parsing mp4 clip with corrupted sample atoms due to improper validation of index in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables in APQ8009, APQ8017, APQ8053, APQ8096AU, APQ8098, Kamorta,	https://www.qualcomm.com/company/product-security/bulletins/july-2020-bulletin	O-QUA-QCS4-190820/812

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			MDM9206, MDM9207C, MDM9607, MSM8905, MSM8909W, MSM8917, MSM8920, MSM8937, MSM8940, MSM8953, MSM8996, MSM8996AU, MSM8998, Nicobar, QCA6574AU, QCM2150, QCS405, QCS605, QM215, Rennell, SA6155P, Saipan, SDA660, SDA845, SDM429, SDM429W, SDM439, SDM450, SDM630, SDM632, SDM636, SDM660, SDM670, SDM710, SDM845, SDX20, SM6150, SM7150, SM8150, SM8250, SXR1130, SXR2130 **CVE ID : CVE-2020-3688**		
Out-of-bounds Write	30-Jul-20	7.5	Out of bound write while QoS DSCP mapping due to improper input validation for data received from association response frame 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, APQ8098, MDM9150, MDM9206, MDM9207C, MDM9607, MDM9650, MSM8905, MSM8909W, MSM8917, MSM8920,	https://www.qualcomm.com/company/product-security/bulletins/july-2020-bulletin	O-QUA-QCS4-190820/813

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			MSM8937, MSM8940, MSM8953, MSM8996AU, Nicobar, QCA6174A, QCA6574AU, QCA9377, QCA9379, QCM2150, QCN7605, QCS405, QCS605, QM215, SA6155P, Saipan, SC8180X, SDA845, SDM429, SDM429W, SDM439, SDM450, SDM630, SDM632, SDM636, SDM660, SDM845, SDX20, SDX55, SM8150, SM8250, SXR2130 **CVE ID : CVE-2020-3698**		
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	30-Jul-20	7.5	Possible out of bound access while processing assoc response from host due to improper length check before copying into buffer 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, Nicobar, QCA6174A, QCA6574AU, QCA9377, QCA9379,	https://www.qualcomm.com/company/product-security/bulletins/july-2020-bulletin	O-QUA-QCS4-190820/814

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			QCM2150, QCN7605, QCS405, QCS605, QM215, SA6155P, Saipan, SC8180X, SDA845, SDM429, SDM429W, SDM439, SDM450, SDM630, SDM632, SDM636, SDM660, SDM845, SDX20, SDX55, SM6150, SM7150, SM8150, SM8250, SXR2130 **CVE ID : CVE-2020-3699**		
ipq4019_firmware					
Out-of-bounds Read	30-Jul-20	5	Possible out of bounds read due to a missing bounds check and could lead to local information disclosure in the wifi driver with no additional execution privileges needed in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking in APQ8053, APQ8096AU, IPQ4019, IPQ8064, IPQ8074, MDM9607, MSM8909W, MSM8996AU, QCA6574AU, QCA9531, QCA9558, QCA9980, SC8180X, SDM439, SDX55, SM8150, SM8250, SXR2130	https://www.qualcomm.com/company/product-security/bulletins/july-2020-bulletin	O-QUA-IPQ4-190820/815

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2020-3700		
ipq8064_firmware					
Out-of-bounds Read	30-Jul-20	5	Possible out of bounds read due to a missing bounds check and could lead to local information disclosure in the wifi driver with no additional execution privileges needed in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking in APQ8053, APQ8096AU, IPQ4019, IPQ8064, IPQ8074, MDM9607, MSM8909W, MSM8996AU, QCA6574AU, QCA9531, QCA9558, QCA9980, SC8180X, SDM439, SDX55, SM8150, SM8250, SXR2130 **CVE ID : CVE-2020-3700**	https://www.qualcomm.com/company/product-security/bulletins/july-2020-bulletin	O-QUA-IPQ8-190820/816
ipq8074_firmware					
Out-of-bounds Read	30-Jul-20	5	Possible out of bounds read due to a missing bounds check and could lead to local information disclosure in the wifi driver with no additional execution privileges needed in Snapdragon Auto, Snapdragon Compute, Snapdragon	https://www.qualcomm.com/company/product-security/bulletins/july-2020-bulletin	O-QUA-IPQ8-190820/817

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Connectivity, Snapdragon Consumer IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking in APQ8053, APQ8096AU, IPQ4019, IPQ8064, IPQ8074, MDM9607, MSM8909W, MSM8996AU, QCA6574AU, QCA9531, QCA9558, QCA9980, SC8180X, SDM439, SDX55, SM8150, SM8250, SXR2130 **CVE ID : CVE-2020-3700**		
qca6174a_firmware					
Out-of-bounds Write	30-Jul-20	7.5	Out of bound write while QoS DSCP mapping due to improper input validation for data received from association response frame 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, APQ8098, MDM9150, MDM9206, MDM9207C, MDM9607, MDM9650, MSM8905, MSM8909W, MSM8917, MSM8920, MSM8937, MSM8940,	https://www.qualcomm.com/company/product-security/bulletins/july-2020-bulletin	O-QUA-QCA6-190820/818

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			MSM8953, MSM8996AU, Nicobar, QCA6174A, QCA6574AU, QCA9377, QCA9379, QCM2150, QCN7605, QCS405, QCS605, QM215, SA6155P, Saipan, SC8180X, SDA845, SDM429, SDM429W, SDM439, SDM450, SDM630, SDM632, SDM636, SDM660, SDM845, SDX20, SDX55, SM8150, SM8250, SXR2130 **CVE ID : CVE-2020-3698**		
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	30-Jul-20	7.5	Possible out of bound access while processing assoc response from host due to improper length check before copying into buffer 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, Nicobar, QCA6174A, QCA6574AU, QCA9377, QCA9379, QCM2150, QCN7605,	https://www.qualcomm.com/company/product-security/bulletins/july-2020-bulletin	O-QUA-QCA6-190820/819

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			QCS405, QCS605, QM215, SA6155P, Saipan, SC8180X, SDA845, SDM429, SDM429W, SDM439, SDM450, SDM630, SDM632, SDM636, SDM660, SDM845, SDX20, SDX55, SM6150, SM7150, SM8150, SM8250, SXR2130 **CVE ID : CVE-2020-3699**		
qca9377_firmware					
Out-of-bounds Write	30-Jul-20	7.5	Out of bound write while QoS DSCP mapping due to improper input validation for data received from association response frame 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, APQ8098, MDM9150, MDM9206, MDM9207C, MDM9607, MDM9650, MSM8905, MSM8909W, MSM8917, MSM8920, MSM8937, MSM8940, MSM8953, MSM8996AU, Nicobar, QCA6174A, QCA6574AU, QCA9377, QCA9379, QCM2150, QCN7605, QCS405,	https://www.qualcomm.com/company/product-security/bulletins/july-2020-bulletin	O-QUA-QCA9-190820/820

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			QCS605, QM215, SA6155P, Saipan, SC8180X, SDA845, SDM429, SDM429W, SDM439, SDM450, SDM630, SDM632, SDM636, SDM660, SDM845, SDX20, SDX55, SM8150, SM8250, SXR2130 **CVE ID : CVE-2020-3698**		
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	30-Jul-20	7.5	Possible out of bound access while processing assoc response from host due to improper length check before copying into buffer 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, Nicobar, QCA6174A, QCA6574AU, QCA9377, QCA9379, QCM2150, QCN7605, QCS405, QCS605, QM215, SA6155P, Saipan, SC8180X, SDA845, SDM429, SDM429W, SDM439, SDM450,	https://www.qualcomm.com/company/product-security/bulletins/july-2020-bulletin	O-QUA-QCA9-190820/821

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			SDM630, SDM632, SDM636, SDM660, SDM845, SDX20, SDX55, SM6150, SM7150, SM8150, SM8250, SXR2130 **CVE ID : CVE-2020-3699**		
qca9379_firmware					
Out-of-bounds Write	30-Jul-20	7.5	Out of bound write while QoS DSCP mapping due to improper input validation for data received from association response frame 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, APQ8098, MDM9150, MDM9206, MDM9207C, MDM9607, MDM9650, MSM8905, MSM8909W, MSM8917, MSM8920, MSM8937, MSM8940, MSM8953, MSM8996AU, Nicobar, QCA6174A, QCA6574AU, QCA9377, QCA9379, QCM2150, QCN7605, QCS405, QCS605, QM215, SA6155P, Saipan, SC8180X, SDA845, SDM429, SDM429W, SDM439, SDM450, SDM630, SDM632,	https://www.qualcomm.com/company/product-security/bulletins/july-2020-bulletin	O-QUA-QCA9-190820/822

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			SDM636, SDM660, SDM845, SDX20, SDX55, SM8150, SM8250, SXR2130 **CVE ID : CVE-2020-3698**		
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	30-Jul-20	7.5	Possible out of bound access while processing assoc response from host due to improper length check before copying into buffer 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, Nicobar, QCA6174A, QCA6574AU, QCA9377, QCA9379, QCM2150, QCN7605, QCS405, QCS605, QM215, SA6155P, Saipan, SC8180X, SDA845, SDM429, SDM429W, SDM439, SDM450, SDM630, SDM632, SDM636, SDM660, SDM845, SDX20, SDX55, SM6150, SM7150, SM8150, SM8250,	https://www.qualcomm.com/company/product-security/bulletins/july-2020-bulletin	O-QUA-QCA9-190820/823

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			SXR2130 **CVE ID : CVE-2020-3699**		
sdm429w_firmware					
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	30-Jul-20	7.5	Possible buffer overflow while parsing mp4 clip with corrupted sample atoms due to improper validation of index in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables in APQ8009, APQ8017, APQ8053, APQ8096AU, APQ8098, Kamorta, MDM9206, MDM9207C, MDM9607, MSM8905, MSM8909W, MSM8917, MSM8920, MSM8937, MSM8940, MSM8953, MSM8996, MSM8996AU, MSM8998, Nicobar, QCA6574AU, QCM2150, QCS405, QCS605, QM215, Rennell, SA6155P, Saipan, SDA660, SDA845, SDM429, SDM429W, SDM439, SDM450, SDM630, SDM632, SDM636, SDM660, SDM670, SDM710, SDM845, SDX20, SM6150, SM7150, SM8150, SM8250, SXR1130, SXR2130 **CVE ID : CVE-2020-3688**	https://www.qualcomm.com/company/product-security/bulletins/july-2020-bulletin	O-QUA-SDM4-190820/824

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Out-of-bounds Write	30-Jul-20	7.5	Out of bound write while QoS DSCP mapping due to improper input validation for data received from association response frame 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, APQ8098, MDM9150, MDM9206, MDM9207C, MDM9607, MDM9650, MSM8905, MSM8909W, MSM8917, MSM8920, MSM8937, MSM8940, MSM8953, MSM8996AU, Nicobar, QCA6174A, QCA6574AU, QCA9377, QCA9379, QCM2150, QCN7605, QCS405, QCS605, QM215, SA6155P, Saipan, SC8180X, SDA845, SDM429, SDM429W, SDM439, SDM450, SDM630, SDM632, SDM636, SDM660, SDM845, SDX20, SDX55, SM8150, SM8250, SXR2130 **CVE ID : CVE-2020-3698**	https://www.qualcomm.com/company/product-security/bulletins/july-2020-bulletin	O-QUA-SDM4-190820/825
Buffer Copy without Checking Size of Input	30-Jul-20	7.5	Possible out of bound access while processing assoc response from host due to improper length	https://www.qualcomm.com/company/product-	O-QUA-SDM4-190820/826

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
('Classic Buffer Overflow')			check before copying into buffer 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, Nicobar, QCA6174A, QCA6574AU, QCA9377, QCA9379, QCM2150, QCN7605, QCS405, QCS605, QM215, SA6155P, Saipan, SC8180X, SDA845, SDM429, SDM429W, SDM439, SDM450, SDM630, SDM632, SDM636, SDM660, SDM845, SDX20, SDX55, SM6150, SM7150, SM8150, SM8250, SXR2130 **CVE ID : CVE-2020-3699**	security/bulletins/july-2020-bulletin	
apq8009_firmware					
Use After Free	30-Jul-20	7.5	Use-after-free issue could occur due to dangling pointer when generating a frame buffer in OpenGL ES in Snapdragon Compute,	https://www.qualcomm.com/company/product-security/bull	O-QUA-APQ8-190820/827

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music in APQ8009, Nicobar, QCM2150, QCS405, Saipan, SDM845, SM8150, SM8250, SXR2130 **CVE ID : CVE-2020-3671**	etins/july-2020-bulletin	
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	30-Jul-20	7.5	Possible buffer overflow while parsing mp4 clip with corrupted sample atoms due to improper validation of index in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables in APQ8009, APQ8017, APQ8053, APQ8096AU, APQ8098, Kamorta, MDM9206, MDM9207C, MDM9607, MSM8905, MSM8909W, MSM8917, MSM8920, MSM8937, MSM8940, MSM8953, MSM8996, MSM8996AU, MSM8998, Nicobar, QCA6574AU, QCM2150, QCS405, QCS605, QM215, Rennell, SA6155P, Saipan, SDA660, SDA845, SDM429, SDM429W, SDM439, SDM450, SDM630, SDM632, SDM636, SDM660, SDM670, SDM710, SDM845, SDX20,	https://www.qualcomm.com/company/product-security/bulletins/july-2020-bulletin	O-QUA-APQ8-190820/828

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			SM6150, SM7150, SM8150, SM8250, SXR1130, SXR2130 **CVE ID : CVE-2020-3688**		
Out-of-bounds Write	30-Jul-20	7.5	Out of bound write while QoS DSCP mapping due to improper input validation for data received from association response frame 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, APQ8098, MDM9150, MDM9206, MDM9207C, MDM9607, MDM9650, MSM8905, MSM8909W, MSM8917, MSM8920, MSM8937, MSM8940, MSM8953, MSM8996AU, Nicobar, QCA6174A, QCA6574AU, QCA9377, QCA9379, QCM2150, QCN7605, QCS405, QCS605, QM215, SA6155P, Saipan, SC8180X, SDA845, SDM429, SDM429W, SDM439, SDM450, SDM630, SDM632, SDM636, SDM660, SDM845, SDX20, SDX55, SM8150, SM8250, SXR2130	https://www.qualcomm.com/company/product-security/bulletins/july-2020-bulletin	O-QUA-APQ8-190820/829

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2020-3698		
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	30-Jul-20	7.5	Possible out of bound access while processing assoc response from host due to improper length check before copying into buffer 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, Nicobar, QCA6174A, QCA6574AU, QCA9377, QCA9379, QCM2150, QCN7605, QCS405, QCS605, QM215, SA6155P, Saipan, SC8180X, SDA845, SDM429, SDM429W, SDM439, SDM450, SDM630, SDM632, SDM636, SDM660, SDM845, SDX20, SDX55, SM6150, SM7150, SM8150, SM8250, SXR2130 **CVE ID : CVE-2020-3699**	https://www.qualcomm.com/company/product-security/bulletins/july-2020-bulletin	O-QUA-APQ8-190820/830
apq8098_firmware					

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	30-Jul-20	7.5	Possible buffer overflow while parsing mp4 clip with corrupted sample atoms due to improper validation of index in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables in APQ8009, APQ8017, APQ8053, APQ8096AU, APQ8098, Kamorta, MDM9206, MDM9207C, MDM9607, MSM8905, MSM8909W, MSM8917, MSM8920, MSM8937, MSM8940, MSM8953, MSM8996, MSM8996AU, MSM8998, Nicobar, QCA6574AU, QCM2150, QCS405, QCS605, QM215, Rennell, SA6155P, Saipan, SDA660, SDA845, SDM429, SDM429W, SDM439, SDM450, SDM630, SDM632, SDM636, SDM660, SDM670, SDM710, SDM845, SDX20, SM6150, SM7150, SM8150, SM8250, SXR1130, SXR2130 **CVE ID : CVE-2020-3688**	https://www.qualcomm.com/company/product-security/bulletins/july-2020-bulletin	O-QUA-APQ8-190820/831
Out-of-bounds Write	30-Jul-20	7.5	Out of bound write while QoS DSCP mapping due to improper input validation for data received from association response	https://www.qualcomm.com/company/product-security/bull	O-QUA-APQ8-190820/832

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			frame 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, APQ8098, MDM9150, MDM9206, MDM9207C, MDM9607, MDM9650, MSM8905, MSM8909W, MSM8917, MSM8920, MSM8937, MSM8940, MSM8953, MSM8996AU, Nicobar, QCA6174A, QCA6574AU, QCA9377, QCA9379, QCM2150, QCN7605, QCS405, QCS605, QM215, SA6155P, Saipan, SC8180X, SDA845, SDM429, SDM429W, SDM439, SDM450, SDM630, SDM632, SDM636, SDM660, SDM845, SDX20, SDX55, SM8150, SM8250, SXR2130 **CVE ID : CVE-2020-3698**	etins/july-2020-bulletin	
msm8953_firmware					
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	30-Jul-20	7.5	Possible buffer overflow while parsing mp4 clip with corrupted sample atoms due to improper validation of index in Snapdragon Auto, Snapdragon Compute,	https://www.qualcomm.com/company/product-security/bulletins/july-2020-	O-QUA-MSM8-190820/833

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables in APQ8009, APQ8017, APQ8053, APQ8096AU, APQ8098, Kamorta, MDM9206, MDM9207C, MDM9607, MSM8905, MSM8909W, MSM8917, MSM8920, MSM8937, MSM8940, MSM8953, MSM8996, MSM8996AU, MSM8998, Nicobar, QCA6574AU, QCM2150, QCS405, QCS605, QM215, Rennell, SA6155P, Saipan, SDA660, SDA845, SDM429, SDM429W, SDM439, SDM450, SDM630, SDM632, SDM636, SDM660, SDM670, SDM710, SDM845, SDX20, SM6150, SM7150, SM8150, SM8250, SXR1130, SXR2130 **CVE ID : CVE-2020-3688**	bulletin	
Out-of-bounds Write	30-Jul-20	7.5	Out of bound write while QoS DSCP mapping due to improper input validation for data received from association response frame in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile,	https://www.qualcomm.com/company/product-security/bulletins/july-2020-bulletin	O-QUA-MSM8-190820/834

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Snapdragon Voice & Music, Snapdragon Wearables in APQ8009, APQ8017, APQ8053, APQ8096AU, APQ8098, MDM9150, MDM9206, MDM9207C, MDM9607, MDM9650, MSM8905, MSM8909W, MSM8917, MSM8920, MSM8937, MSM8940, MSM8953, MSM8996AU, Nicobar, QCA6174A, QCA6574AU, QCA9377, QCA9379, QCM2150, QCN7605, QCS405, QCS605, QM215, SA6155P, Saipan, SC8180X, SDA845, SDM429, SDM429W, SDM439, SDM450, SDM630, SDM632, SDM636, SDM660, SDM845, SDX20, SDX55, SM8150, SM8250, SXR2130 **CVE ID : CVE-2020-3698**		
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	30-Jul-20	7.5	Possible out of bound access while processing assoc response from host due to improper length check before copying into buffer 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,	https://www.qualcomm.com/company/product-security/bulletins/july-2020-bulletin	O-QUA-MSM8-190820/835

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			MDM9206, MDM9207C, MDM9607, MDM9640, MDM9650, MSM8905, MSM8909W, MSM8917, MSM8920, MSM8937, MSM8940, MSM8953, MSM8996AU, Nicobar, QCA6174A, QCA6574AU, QCA9377, QCA9379, QCM2150, QCN7605, QCS405, QCS605, QM215, SA6155P, Saipan, SC8180X, SDA845, SDM429, SDM429W, SDM439, SDM450, SDM630, SDM632, SDM636, SDM660, SDM845, SDX20, SDX55, SM6150, SM7150, SM8150, SM8250, SXR2130 **CVE ID : CVE-2020-3699**		
msm8998_firmware					
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	30-Jul-20	7.5	Possible buffer overflow while parsing mp4 clip with corrupted sample atoms due to improper validation of index in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables in APQ8009, APQ8017, APQ8053, APQ8096AU, APQ8098, Kamorta, MDM9206, MDM9207C,	https://www.qualcomm.com/company/product-security/bulletins/july-2020-bulletin	O-QUA-MSM8-190820/836

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			MDM9607, MSM8905, MSM8909W, MSM8917, MSM8920, MSM8937, MSM8940, MSM8953, MSM8996, MSM8996AU, MSM8998, Nicobar, QCA6574AU, QCM2150, QCS405, QCS605, QM215, Rennell, SA6155P, Saipan, SDA660, SDA845, SDM429, SDM429W, SDM439, SDM450, SDM630, SDM632, SDM636, SDM660, SDM670, SDM710, SDM845, SDX20, SM6150, SM7150, SM8150, SM8250, SXR1130, SXR2130 **CVE ID : CVE-2020-3688**		
nicobar_firmware					
Use After Free	30-Jul-20	7.5	Use-after-free issue could occur due to dangling pointer when generating a frame buffer in OpenGL ES in Snapdragon Compute, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music in APQ8009, Nicobar, QCM2150, QCS405, Saipan, SDM845, SM8150, SM8250, SXR2130 **CVE ID : CVE-2020-3671**	https://www.qualcomm.com/company/product-security/bulletins/july-2020-bulletin	O-QUA-NICO-190820/837
Buffer Copy without Checking Size of Input ('Classic Buffer	30-Jul-20	7.5	Possible buffer overflow while parsing mp4 clip with corrupted sample atoms due to improper validation of index in Snapdragon Auto,	https://www.qualcomm.com/company/product-security/bulletins/july-	O-QUA-NICO-190820/838

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Overflow')			Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables in APQ8009, APQ8017, APQ8053, APQ8096AU, APQ8098, Kamorta, MDM9206, MDM9207C, MDM9607, MSM8905, MSM8909W, MSM8917, MSM8920, MSM8937, MSM8940, MSM8953, MSM8996, MSM8996AU, MSM8998, Nicobar, QCA6574AU, QCM2150, QCS405, QCS605, QM215, Rennell, SA6155P, Saipan, SDA660, SDA845, SDM429, SDM429W, SDM439, SDM450, SDM630, SDM632, SDM636, SDM660, SDM670, SDM710, SDM845, SDX20, SM6150, SM7150, SM8150, SM8250, SXR1130, SXR2130 **CVE ID : CVE-2020-3688**	2020-bulletin	
Out-of-bounds Write	30-Jul-20	7.5	Out of bound write while QoS DSCP mapping due to improper input validation for data received from association response frame in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial	https://www.qualcomm.com/company/product-security/bulletins/july-2020-bulletin	O-QUA-NICO-190820/839

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables in APQ8009, APQ8017, APQ8053, APQ8096AU, APQ8098, MDM9150, MDM9206, MDM9207C, MDM9607, MDM9650, MSM8905, MSM8909W, MSM8917, MSM8920, MSM8937, MSM8940, MSM8953, MSM8996AU, Nicobar, QCA6174A, QCA6574AU, QCA9377, QCA9379, QCM2150, QCN7605, QCS405, QCS605, QM215, SA6155P, Saipan, SC8180X, SDA845, SDM429, SDM429W, SDM439, SDM450, SDM630, SDM632, SDM636, SDM660, SDM845, SDX20, SDX55, SM8150, SM8250, SXR2130 **CVE ID : CVE-2020-3698**		
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	30-Jul-20	7.5	Possible out of bound access while processing assoc response from host due to improper length check before copying into buffer 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,	https://www.qualcomm.com/company/product-security/bulletins/july-2020-bulletin	O-QUA-NICO-190820/840

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			APQ8053, APQ8096AU, MDM9206, MDM9207C, MDM9607, MDM9640, MDM9650, MSM8905, MSM8909W, MSM8917, MSM8920, MSM8937, MSM8940, MSM8953, MSM8996AU, Nicobar, QCA6174A, QCA6574AU, QCA9377, QCA9379, QCM2150, QCN7605, QCS405, QCS605, QM215, SA6155P, Saipan, SC8180X, SDA845, SDM429, SDM429W, SDM439, SDM450, SDM630, SDM632, SDM636, SDM660, SDM845, SDX20, SDX55, SM6150, SM7150, SM8150, SM8250, SXR2130 **CVE ID : CVE-2020-3699**		
apq8053_firmware					
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	30-Jul-20	7.5	Possible buffer overflow while parsing mp4 clip with corrupted sample atoms due to improper validation of index in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables in APQ8009, APQ8017, APQ8053, APQ8096AU, APQ8098, Kamorta,	https://www.qualcomm.com/company/product-security/bulletins/july-2020-bulletin	O-QUA-APQ8-190820/841

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			MDM9206, MDM9207C, MDM9607, MSM8905, MSM8909W, MSM8917, MSM8920, MSM8937, MSM8940, MSM8953, MSM8996, MSM8996AU, MSM8998, Nicobar, QCA6574AU, QCM2150, QCS405, QCS605, QM215, Rennell, SA6155P, Saipan, SDA660, SDA845, SDM429, SDM429W, SDM439, SDM450, SDM630, SDM632, SDM636, SDM660, SDM670, SDM710, SDM845, SDX20, SM6150, SM7150, SM8150, SM8250, SXR1130, SXR2130 **CVE ID : CVE-2020-3688**		
Out-of-bounds Write	30-Jul-20	7.5	Out of bound write while QoS DSCP mapping due to improper input validation for data received from association response frame 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, APQ8098, MDM9150, MDM9206, MDM9207C, MDM9607, MDM9650, MSM8905, MSM8909W, MSM8917, MSM8920,	https://www.qualcomm.com/company/product-security/bulletins/july-2020-bulletin	O-QUA-APQ8-190820/842

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			MSM8937, MSM8940, MSM8953, MSM8996AU, Nicobar, QCA6174A, QCA6574AU, QCA9377, QCA9379, QCM2150, QCN7605, QCS405, QCS605, QM215, SA6155P, Saipan, SC8180X, SDA845, SDM429, SDM429W, SDM439, SDM450, SDM630, SDM632, SDM636, SDM660, SDM845, SDX20, SDX55, SM8150, SM8250, SXR2130 **CVE ID : CVE-2020-3698**		
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	30-Jul-20	7.5	Possible out of bound access while processing assoc response from host due to improper length check before copying into buffer 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, Nicobar, QCA6174A, QCA6574AU, QCA9377, QCA9379,	https://www.qualcomm.com/company/product-security/bulletins/july-2020-bulletin	O-QUA-APQ8-190820/843

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			QCM2150, QCN7605, QCS405, QCS605, QM215, SA6155P, Saipan, SC8180X, SDA845, SDM429, SDM429W, SDM439, SDM450, SDM630, SDM632, SDM636, SDM660, SDM845, SDX20, SDX55, SM6150, SM7150, SM8150, SM8250, SXR2130 **CVE ID : CVE-2020-3699**		
Out-of-bounds Read	30-Jul-20	5	Possible out of bounds read due to a missing bounds check and could lead to local information disclosure in the wifi driver with no additional execution privileges needed in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking in APQ8053, APQ8096AU, IPQ4019, IPQ8064, IPQ8074, MDM9607, MSM8909W, MSM8996AU, QCA6574AU, QCA9531, QCA9558, QCA9980, SC8180X, SDM439, SDX55, SM8150, SM8250, SXR2130 **CVE ID : CVE-2020-3700**	https://www.qualcomm.com/company/product-security/bulletins/july-2020-bulletin	O-QUA-APQ8-190820/844

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
mdm9207c_firmware					
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	30-Jul-20	7.5	Possible buffer overflow while parsing mp4 clip with corrupted sample atoms due to improper validation of index in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables in APQ8009, APQ8017, APQ8053, APQ8096AU, APQ8098, Kamorta, MDM9206, MDM9207C, MDM9607, MSM8905, MSM8909W, MSM8917, MSM8920, MSM8937, MSM8940, MSM8953, MSM8996, MSM8996AU, MSM8998, Nicobar, QCA6574AU, QCM2150, QCS405, QCS605, QM215, Rennell, SA6155P, Saipan, SDA660, SDA845, SDM429, SDM429W, SDM439, SDM450, SDM630, SDM632, SDM636, SDM660, SDM670, SDM710, SDM845, SDX20, SM6150, SM7150, SM8150, SM8250, SXR1130, SXR2130 **CVE ID : CVE-2020-3688**	https://www.qualcomm.com/company/product-security/bulletins/july-2020-bulletin	O-QUA-MDM9-190820/845
Out-of-bounds Write	30-Jul-20	7.5	Out of bound write while QoS DSCP mapping due to improper input validation	https://www.qualcomm.com/compan	O-QUA-MDM9-190820/846

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			for data received from association response frame 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, APQ8098, MDM9150, MDM9206, MDM9207C, MDM9607, MDM9650, MSM8905, MSM8909W, MSM8917, MSM8920, MSM8937, MSM8940, MSM8953, MSM8996AU, Nicobar, QCA6174A, QCA6574AU, QCA9377, QCA9379, QCM2150, QCN7605, QCS405, QCS605, QM215, SA6155P, Saipan, SC8180X, SDA845, SDM429, SDM429W, SDM439, SDM450, SDM630, SDM632, SDM636, SDM660, SDM845, SDX20, SDX55, SM8150, SM8250, SXR2130 **CVE ID : CVE-2020-3698**	y/product-security/bulletins/july-2020-bulletin	
Buffer Copy without Checking Size of Input ('Classic Buffer	30-Jul-20	7.5	Possible out of bound access while processing assoc response from host due to improper length check before copying into buffer in Snapdragon Auto, Snapdragon Compute,	https://www.qualcomm.com/company/product-security/bulletins/july-2020-	O-QUA-MDM9-190820/847

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Overflow')			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, Nicobar, QCA6174A, QCA6574AU, QCA9377, QCA9379, QCM2150, QCN7605, QCS405, QCS605, QM215, SA6155P, Saipan, SC8180X, SDA845, SDM429, SDM429W, SDM439, SDM450, SDM630, SDM632, SDM636, SDM660, SDM845, SDX20, SDX55, SM6150, SM7150, SM8150, SM8250, SXR2130 **CVE ID : CVE-2020-3699**	bulletin	
msm8905_firmware					
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	30-Jul-20	7.5	Possible buffer overflow while parsing mp4 clip with corrupted sample atoms due to improper validation of index in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity,	https://www.qualcomm.com/company/product-security/bulletins/july-2020-bulletin	O-QUA-MSM8-190820/848

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, APQ8098, Kamorta, MDM9206, MDM9207C, MDM9607, MSM8905, MSM8909W, MSM8917, MSM8920, MSM8937, MSM8940, MSM8953, MSM8996, MSM8996AU, MSM8998, Nicobar, QCA6574AU, QCM2150, QCS405, QCS605, QM215, Rennell, SA6155P, Saipan, SDA660, SDA845, SDM429, SDM429W, SDM439, SDM450, SDM630, SDM632, SDM636, SDM660, SDM670, SDM710, SDM845, SDX20, SM6150, SM7150, SM8150, SM8250, SXR1130, SXR2130 **CVE ID : CVE-2020-3688**		
Out-of-bounds Write	30-Jul-20	7.5	Out of bound write while QoS DSCP mapping due to improper input validation for data received from association response frame in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music,	https://www.qualcomm.com/company/product-security/bulletins/july-2020-bulletin	O-QUA-MSM8-190820/849

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Snapdragon Wearables in APQ8009, APQ8017, APQ8053, APQ8096AU, APQ8098, MDM9150, MDM9206, MDM9207C, MDM9607, MDM9650, MSM8905, MSM8909W, MSM8917, MSM8920, MSM8937, MSM8940, MSM8953, MSM8996AU, Nicobar, QCA6174A, QCA6574AU, QCA9377, QCA9379, QCM2150, QCN7605, QCS405, QCS605, QM215, SA6155P, Saipan, SC8180X, SDA845, SDM429, SDM429W, SDM439, SDM450, SDM630, SDM632, SDM636, SDM660, SDM845, SDX20, SDX55, SM8150, SM8250, SXR2130 **CVE ID : CVE-2020-3698**		
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	30-Jul-20	7.5	Possible out of bound access while processing assoc response from host due to improper length check before copying into buffer 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,	https://www.qualcomm.com/company/product-security/bulletins/july-2020-bulletin	O-QUA-MSM8-190820/850

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			MDM9607, MDM9640, MDM9650, MSM8905, MSM8909W, MSM8917, MSM8920, MSM8937, MSM8940, MSM8953, MSM8996AU, Nicobar, QCA6174A, QCA6574AU, QCA9377, QCA9379, QCM2150, QCN7605, QCS405, QCS605, QM215, SA6155P, Saipan, SC8180X, SDA845, SDM429, SDM429W, SDM439, SDM450, SDM630, SDM632, SDM636, SDM660, SDM845, SDX20, SDX55, SM6150, SM7150, SM8150, SM8250, SXR2130 **CVE ID : CVE-2020-3699**		
qcn7605_firmware					
Out-of-bounds Write	30-Jul-20	7.5	Out of bound write while QoS DSCP mapping due to improper input validation for data received from association response frame 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, APQ8098, MDM9150, MDM9206, MDM9207C,	https://www.qualcomm.com/company/product-security/bulletins/july-2020-bulletin	O-QUA-QCN7-190820/851

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			MDM9607, MDM9650, MSM8905, MSM8909W, MSM8917, MSM8920, MSM8937, MSM8940, MSM8953, MSM8996AU, Nicobar, QCA6174A, QCA6574AU, QCA9377, QCA9379, QCM2150, QCN7605, QCS405, QCS605, QM215, SA6155P, Saipan, SC8180X, SDA845, SDM429, SDM429W, SDM439, SDM450, SDM630, SDM632, SDM636, SDM660, SDM845, SDX20, SDX55, SM8150, SM8250, SXR2130 **CVE ID : CVE-2020-3698**		
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	30-Jul-20	7.5	Possible out of bound access while processing assoc response from host due to improper length check before copying into buffer 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,	https://www.qualcomm.com/company/product-security/bulletins/july-2020-bulletin	O-QUA-QCN7-190820/852

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			MSM8996AU, Nicobar, QCA6174A, QCA6574AU, QCA9377, QCA9379, QCM2150, QCN7605, QCS405, QCS605, QM215, SA6155P, Saipan, SC8180X, SDA845, SDM429, SDM429W, SDM439, SDM450, SDM630, SDM632, SDM636, SDM660, SDM845, SDX20, SDX55, SM6150, SM7150, SM8150, SM8250, SXR2130 **CVE ID : CVE-2020-3699**		
sdm845_firmware					
Use After Free	30-Jul-20	7.5	Use-after-free issue could occur due to dangling pointer when generating a frame buffer in OpenGL ES in Snapdragon Compute, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music in APQ8009, Nicobar, QCM2150, QCS405, Saipan, SDM845, SM8150, SM8250, SXR2130 **CVE ID : CVE-2020-3671**	https://www.qualcomm.com/company/product-security/bulletins/july-2020-bulletin	O-QUA-SDM8-190820/853
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	30-Jul-20	7.5	Possible buffer overflow while parsing mp4 clip with corrupted sample atoms due to improper validation of index in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer	https://www.qualcomm.com/company/product-security/bulletins/july-2020-bulletin	O-QUA-SDM8-190820/854

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables in APQ8009, APQ8017, APQ8053, APQ8096AU, APQ8098, Kamorta, MDM9206, MDM9207C, MDM9607, MSM8905, MSM8909W, MSM8917, MSM8920, MSM8937, MSM8940, MSM8953, MSM8996, MSM8996AU, MSM8998, Nicobar, QCA6574AU, QCM2150, QCS405, QCS605, QM215, Rennell, SA6155P, Saipan, SDA660, SDA845, SDM429, SDM429W, SDM439, SDM450, SDM630, SDM632, SDM636, SDM660, SDM670, SDM710, SDM845, SDX20, SM6150, SM7150, SM8150, SM8250, SXR1130, SXR2130 **CVE ID : CVE-2020-3688**		
Out-of-bounds Write	30-Jul-20	7.5	Out of bound write while QoS DSCP mapping due to improper input validation for data received from association response frame in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables in	https://www.qualcomm.com/company/product-security/bulletins/july-2020-bulletin	O-QUA-SDM8-190820/855

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			APQ8009, APQ8017, APQ8053, APQ8096AU, APQ8098, MDM9150, MDM9206, MDM9207C, MDM9607, MDM9650, MSM8905, MSM8909W, MSM8917, MSM8920, MSM8937, MSM8940, MSM8953, MSM8996AU, Nicobar, QCA6174A, QCA6574AU, QCA9377, QCA9379, QCM2150, QCN7605, QCS405, QCS605, QM215, SA6155P, Saipan, SC8180X, SDA845, SDM429, SDM429W, SDM439, SDM450, SDM630, SDM632, SDM636, SDM660, SDM845, SDX20, SDX55, SM8150, SM8250, SXR2130 **CVE ID : CVE-2020-3698**		
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	30-Jul-20	7.5	Possible out of bound access while processing assoc response from host due to improper length check before copying into buffer 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,	https://www.qualcomm.com/company/product-security/bulletins/july-2020-bulletin	O-QUA-SDM8-190820/856

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			MDM9650, MSM8905, MSM8909W, MSM8917, MSM8920, MSM8937, MSM8940, MSM8953, MSM8996AU, Nicobar, QCA6174A, QCA6574AU, QCA9377, QCA9379, QCM2150, QCN7605, QCS405, QCS605, QM215, SA6155P, Saipan, SC8180X, SDA845, SDM429, SDM429W, SDM439, SDM450, SDM630, SDM632, SDM636, SDM660, SDM845, SDX20, SDX55, SM6150, SM7150, SM8150, SM8250, SXR2130 **CVE ID : CVE-2020-3699**		
apq8017_firmware					
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	30-Jul-20	7.5	Possible buffer overflow while parsing mp4 clip with corrupted sample atoms due to improper validation of index in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables in APQ8009, APQ8017, APQ8053, APQ8096AU, APQ8098, Kamorta, MDM9206, MDM9207C, MDM9607, MSM8905, MSM8909W, MSM8917,	https://www.qualcomm.com/company/product-security/bulletins/july-2020-bulletin	O-QUA-APQ8-190820/857

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			MSM8920, MSM8937, MSM8940, MSM8953, MSM8996, MSM8996AU, MSM8998, Nicobar, QCA6574AU, QCM2150, QCS405, QCS605, QM215, Rennell, SA6155P, Saipan, SDA660, SDA845, SDM429, SDM429W, SDM439, SDM450, SDM630, SDM632, SDM636, SDM660, SDM670, SDM710, SDM845, SDX20, SM6150, SM7150, SM8150, SM8250, SXR1130, SXR2130 **CVE ID : CVE-2020-3688**		
Out-of-bounds Write	30-Jul-20	7.5	Out of bound write while QoS DSCP mapping due to improper input validation for data received from association response frame 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, APQ8098, MDM9150, MDM9206, MDM9207C, MDM9607, MDM9650, MSM8905, MSM8909W, MSM8917, MSM8920, MSM8937, MSM8940, MSM8953, MSM8996AU, Nicobar, QCA6174A,	https://www.qualcomm.com/company/product-security/bulletins/july-2020-bulletin	O-QUA-APQ8-190820/858

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			QCA6574AU, QCA9377, QCA9379, QCM2150, QCN7605, QCS405, QCS605, QM215, SA6155P, Saipan, SC8180X, SDA845, SDM429, SDM429W, SDM439, SDM450, SDM630, SDM632, SDM636, SDM660, SDM845, SDX20, SDX55, SM8150, SM8250, SXR2130 **CVE ID : CVE-2020-3698**		
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	30-Jul-20	7.5	Possible out of bound access while processing assoc response from host due to improper length check before copying into buffer 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, Nicobar, QCA6174A, QCA6574AU, QCA9377, QCA9379, QCM2150, QCN7605, QCS405, QCS605, QM215, SA6155P, Saipan,	https://www.qualcomm.com/company/product-security/bulletins/july-2020-bulletin	O-QUA-APQ8-190820/859

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			SC8180X, SDA845, SDM429, SDM429W, SDM439, SDM450, SDM630, SDM632, SDM636, SDM660, SDM845, SDX20, SDX55, SM6150, SM7150, SM8150, SM8250, SXR2130 **CVE ID : CVE-2020-3699**		
apq8096au_firmware					
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	30-Jul-20	7.5	Possible buffer overflow while parsing mp4 clip with corrupted sample atoms due to improper validation of index in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables in APQ8009, APQ8017, APQ8053, APQ8096AU, APQ8098, Kamorta, MDM9206, MDM9207C, MDM9607, MSM8905, MSM8909W, MSM8917, MSM8920, MSM8937, MSM8940, MSM8953, MSM8996, MSM8996AU, MSM8998, Nicobar, QCA6574AU, QCM2150, QCS405, QCS605, QM215, Rennell, SA6155P, Saipan, SDA660, SDA845, SDM429, SDM429W, SDM439, SDM450, SDM630,	https://www.qualcomm.com/company/product-security/bulletins/july-2020-bulletin	O-QUA-APQ8-190820/860

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			SDM632, SDM636, SDM660, SDM670, SDM710, SDM845, SDX20, SM6150, SM7150, SM8150, SM8250, SXR1130, SXR2130 **CVE ID : CVE-2020-3688**		
Out-of-bounds Write	30-Jul-20	7.5	Out of bound write while QoS DSCP mapping due to improper input validation for data received from association response frame 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, APQ8098, MDM9150, MDM9206, MDM9207C, MDM9607, MDM9650, MSM8905, MSM8909W, MSM8917, MSM8920, MSM8937, MSM8940, MSM8953, MSM8996AU, Nicobar, QCA6174A, QCA6574AU, QCA9377, QCA9379, QCM2150, QCN7605, QCS405, QCS605, QM215, SA6155P, Saipan, SC8180X, SDA845, SDM429, SDM429W, SDM439, SDM450, SDM630, SDM632, SDM636, SDM660, SDM845, SDX20, SDX55,	https://www.qualcomm.com/company/product-security/bulletins/july-2020-bulletin	O-QUA-APQ8-190820/861

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			SM8150, SM8250, SXR2130 **CVE ID : CVE-2020-3698**		
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	30-Jul-20	7.5	Possible out of bound access while processing assoc response from host due to improper length check before copying into buffer 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, Nicobar, QCA6174A, QCA6574AU, QCA9377, QCA9379, QCM2150, QCN7605, QCS405, QCS605, QM215, SA6155P, Saipan, SC8180X, SDA845, SDM429, SDM429W, SDM439, SDM450, SDM630, SDM632, SDM636, SDM660, SDM845, SDX20, SDX55, SM6150, SM7150, SM8150, SM8250, SXR2130	https://www.qualcomm.com/company/product-security/bulletins/july-2020-bulletin	O-QUA-APQ8-190820/862

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2020-3699		
Out-of-bounds Read	30-Jul-20	5	Possible out of bounds read due to a missing bounds check and could lead to local information disclosure in the wifi driver with no additional execution privileges needed in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking in APQ8053, APQ8096AU, IPQ4019, IPQ8064, IPQ8074, MDM9607, MSM8909W, MSM8996AU, QCA6574AU, QCA9531, QCA9558, QCA9980, SC8180X, SDM439, SDX55, SM8150, SM8250, SXR2130 **CVE ID : CVE-2020-3700**	https://www.qualcomm.com/company/product-security/bulletins/july-2020-bulletin	O-QUA-APQ8-190820/863
sda845_firmware					
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	30-Jul-20	7.5	Possible buffer overflow while parsing mp4 clip with corrupted sample atoms due to improper validation of index in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile,	https://www.qualcomm.com/company/product-security/bulletins/july-2020-bulletin	O-QUA-SDA8-190820/864

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Snapdragon Voice & Music, Snapdragon Wearables in APQ8009, APQ8017, APQ8053, APQ8096AU, APQ8098, Kamorta, MDM9206, MDM9207C, MDM9607, MSM8905, MSM8909W, MSM8917, MSM8920, MSM8937, MSM8940, MSM8953, MSM8996, MSM8996AU, MSM8998, Nicobar, QCA6574AU, QCM2150, QCS405, QCS605, QM215, Rennell, SA6155P, Saipan, SDA660, SDA845, SDM429, SDM429W, SDM439, SDM450, SDM630, SDM632, SDM636, SDM660, SDM670, SDM710, SDM845, SDX20, SM6150, SM7150, SM8150, SM8250, SXR1130, SXR2130 **CVE ID : CVE-2020-3688**		
Out-of-bounds Write	30-Jul-20	7.5	Out of bound write while QoS DSCP mapping due to improper input validation for data received from association response frame 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,	https://www.qualcomm.com/company/product-security/bulletins/july-2020-bulletin	O-QUA-SDA8-190820/865

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			APQ8098, MDM9150, MDM9206, MDM9207C, MDM9607, MDM9650, MSM8905, MSM8909W, MSM8917, MSM8920, MSM8937, MSM8940, MSM8953, MSM8996AU, Nicobar, QCA6174A, QCA6574AU, QCA9377, QCA9379, QCM2150, QCN7605, QCS405, QCS605, QM215, SA6155P, Saipan, SC8180X, SDA845, SDM429, SDM429W, SDM439, SDM450, SDM630, SDM632, SDM636, SDM660, SDM845, SDX20, SDX55, SM8150, SM8250, SXR2130 **CVE ID : CVE-2020-3698**		
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	30-Jul-20	7.5	Possible out of bound access while processing assoc response from host due to improper length check before copying into buffer 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,	https://www.qualcomm.com/company/product-security/bulletins/july-2020-bulletin	O-QUA-SDA8-190820/866

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			MSM8920, MSM8937, MSM8940, MSM8953, MSM8996AU, Nicobar, QCA6174A, QCA6574AU, QCA9377, QCA9379, QCM2150, QCN7605, QCS405, QCS605, QM215, SA6155P, Saipan, SC8180X, SDA845, SDM429, SDM429W, SDM439, SDM450, SDM630, SDM632, SDM636, SDM660, SDM845, SDX20, SDX55, SM6150, SM7150, SM8150, SM8250, SXR2130 **CVE ID : CVE-2020-3699**		
sdm636_firmware					
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	30-Jul-20	7.5	Possible buffer overflow while parsing mp4 clip with corrupted sample atoms due to improper validation of index in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables in APQ8009, APQ8017, APQ8053, APQ8096AU, APQ8098, Kamorta, MDM9206, MDM9207C, MDM9607, MSM8905, MSM8909W, MSM8917, MSM8920, MSM8937, MSM8940, MSM8953,	https://www.qualcomm.com/company/product-security/bulletins/july-2020-bulletin	O-QUA-SDM6-190820/867

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			MSM8996, MSM8996AU, MSM8998, Nicobar, QCA6574AU, QCM2150, QCS405, QCS605, QM215, Rennell, SA6155P, Saipan, SDA660, SDA845, SDM429, SDM429W, SDM439, SDM450, SDM630, SDM632, SDM636, SDM660, SDM670, SDM710, SDM845, SDX20, SM6150, SM7150, SM8150, SM8250, SXR1130, SXR2130 **CVE ID : CVE-2020-3688**		
Out-of-bounds Write	30-Jul-20	7.5	Out of bound write while QoS DSCP mapping due to improper input validation for data received from association response frame 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, APQ8098, MDM9150, MDM9206, MDM9207C, MDM9607, MDM9650, MSM8905, MSM8909W, MSM8917, MSM8920, MSM8937, MSM8940, MSM8953, MSM8996AU, Nicobar, QCA6174A, QCA6574AU, QCA9377, QCA9379, QCM2150,	https://www.qualcomm.com/company/product-security/bulletins/july-2020-bulletin	O-QUA-SDM6-190820/868

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			QCN7605, QCS405, QCS605, QM215, SA6155P, Saipan, SC8180X, SDA845, SDM429, SDM429W, SDM439, SDM450, SDM630, SDM632, SDM636, SDM660, SDM845, SDX20, SDX55, SM8150, SM8250, SXR2130 **CVE ID : CVE-2020-3698**		
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	30-Jul-20	7.5	Possible out of bound access while processing assoc response from host due to improper length check before copying into buffer 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, Nicobar, QCA6174A, QCA6574AU, QCA9377, QCA9379, QCM2150, QCN7605, QCS405, QCS605, QM215, SA6155P, Saipan, SC8180X, SDA845, SDM429, SDM429W,	https://www.qualcomm.com/company/product-security/bulletins/july-2020-bulletin	O-QUA-SDM6-190820/869

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			SDM439, SDM450, SDM630, SDM632, SDM636, SDM660, SDM845, SDX20, SDX55, SM6150, SM7150, SM8150, SM8250, SXR2130 **CVE ID : CVE-2020-3699**		
sdm670_firmware					
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	30-Jul-20	7.5	Possible buffer overflow while parsing mp4 clip with corrupted sample atoms due to improper validation of index in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables in APQ8009, APQ8017, APQ8053, APQ8096AU, APQ8098, Kamorta, MDM9206, MDM9207C, MDM9607, MSM8905, MSM8909W, MSM8917, MSM8920, MSM8937, MSM8940, MSM8953, MSM8996, MSM8996AU, MSM8998, Nicobar, QCA6574AU, QCM2150, QCS405, QCS605, QM215, Rennell, SA6155P, Saipan, SDA660, SDA845, SDM429, SDM429W, SDM439, SDM450, SDM630, SDM632, SDM636, SDM660, SDM670,	https://www.qualcomm.com/company/product-security/bulletins/july-2020-bulletin	O-QUA-SDM6-190820/870

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			SDM710, SDM845, SDX20, SM6150, SM7150, SM8150, SM8250, SXR1130, SXR2130 **CVE ID : CVE-2020-3688**		
sdm710_firmware					
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	30-Jul-20	7.5	Possible buffer overflow while parsing mp4 clip with corrupted sample atoms due to improper validation of index in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables in APQ8009, APQ8017, APQ8053, APQ8096AU, APQ8098, Kamorta, MDM9206, MDM9207C, MDM9607, MSM8905, MSM8909W, MSM8917, MSM8920, MSM8937, MSM8940, MSM8953, MSM8996, MSM8996AU, MSM8998, Nicobar, QCA6574AU, QCM2150, QCS405, QCS605, QM215, Rennell, SA6155P, Saipan, SDA660, SDA845, SDM429, SDM429W, SDM439, SDM450, SDM630, SDM632, SDM636, SDM660, SDM670, SDM710, SDM845, SDX20, SM6150, SM7150, SM8150, SM8250,	https://www.qualcomm.com/company/product-security/bulletins/july-2020-bulletin	O-QUA-SDM7-190820/871

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			SXR1130, SXR2130 **CVE ID : CVE-2020-3688**		
sm6150_firmware					
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	30-Jul-20	7.5	Possible buffer overflow while parsing mp4 clip with corrupted sample atoms due to improper validation of index in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables in APQ8009, APQ8017, APQ8053, APQ8096AU, APQ8098, Kamorta, MDM9206, MDM9207C, MDM9607, MSM8905, MSM8909W, MSM8917, MSM8920, MSM8937, MSM8940, MSM8953, MSM8996, MSM8996AU, MSM8998, Nicobar, QCA6574AU, QCM2150, QCS405, QCS605, QM215, Rennell, SA6155P, Saipan, SDA660, SDA845, SDM429, SDM429W, SDM439, SDM450, SDM630, SDM632, SDM636, SDM660, SDM670, SDM710, SDM845, SDX20, SM6150, SM7150, SM8150, SM8250, SXR1130, SXR2130 **CVE ID : CVE-2020-3688**	https://www.qualcomm.com/company/product-security/bulletins/july-2020-bulletin	O-QUA-SM61-190820/872

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	30-Jul-20	7.5	Possible out of bound access while processing assoc response from host due to improper length check before copying into buffer 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, Nicobar, QCA6174A, QCA6574AU, QCA9377, QCA9379, QCM2150, QCN7605, QCS405, QCS605, QM215, SA6155P, Saipan, SC8180X, SDA845, SDM429, SDM429W, SDM439, SDM450, SDM630, SDM632, SDM636, SDM660, SDM845, SDX20, SDX55, SM6150, SM7150, SM8150, SM8250, SXR2130 **CVE ID : CVE-2020-3699**	https://www.qualcomm.com/company/product-security/bulletins/july-2020-bulletin	O-QUA-SM61-190820/873
qm215_firmware					
Buffer Copy	30-Jul-20	7.5	Possible buffer overflow	https://ww	O-QUA-

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
without Checking Size of Input ('Classic Buffer Overflow')			while parsing mp4 clip with corrupted sample atoms due to improper validation of index in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables in APQ8009, APQ8017, APQ8053, APQ8096AU, APQ8098, Kamorta, MDM9206, MDM9207C, MDM9607, MSM8905, MSM8909W, MSM8917, MSM8920, MSM8937, MSM8940, MSM8953, MSM8996, MSM8996AU, MSM8998, Nicobar, QCA6574AU, QCM2150, QCS405, QCS605, QM215, Rennell, SA6155P, Saipan, SDA660, SDA845, SDM429, SDM429W, SDM439, SDM450, SDM630, SDM632, SDM636, SDM660, SDM670, SDM710, SDM845, SDX20, SM6150, SM7150, SM8150, SM8250, SXR1130, SXR2130 **CVE ID : CVE-2020-3688**	w.qualcomm.com/company/product-security/bulletins/july-2020-bulletin	QM21-190820/874
Out-of-bounds Write	30-Jul-20	7.5	Out of bound write while QoS DSCP mapping due to improper input validation for data received from association response frame in Snapdragon Auto,	https://www.qualcomm.com/company/product-security/bulletins/july-	O-QUA-QM21-190820/875

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Snapdragon Compute, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables in APQ8009, APQ8017, APQ8053, APQ8096AU, APQ8098, MDM9150, MDM9206, MDM9207C, MDM9607, MDM9650, MSM8905, MSM8909W, MSM8917, MSM8920, MSM8937, MSM8940, MSM8953, MSM8996AU, Nicobar, QCA6174A, QCA6574AU, QCA9377, QCA9379, QCM2150, QCN7605, QCS405, QCS605, QM215, SA6155P, Saipan, SC8180X, SDA845, SDM429, SDM429W, SDM439, SDM450, SDM630, SDM632, SDM636, SDM660, SDM845, SDX20, SDX55, SM8150, SM8250, SXR2130 **CVE ID : CVE-2020-3698**	2020-bulletin	
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	30-Jul-20	7.5	Possible out of bound access while processing assoc response from host due to improper length check before copying into buffer in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer	https://www.qualcomm.com/company/product-security/bulletins/july-2020-bulletin	O-QUA-QM21-190820/876

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			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, Nicobar, QCA6174A, QCA6574AU, QCA9377, QCA9379, QCM2150, QCN7605, QCS405, QCS605, QM215, SA6155P, Saipan, SC8180X, SDA845, SDM429, SDM429W, SDM439, SDM450, SDM630, SDM632, SDM636, SDM660, SDM845, SDX20, SDX55, SM6150, SM7150, SM8150, SM8250, SXR2130 **CVE ID : CVE-2020-3699**		
sm8150_firmware					
Use After Free	30-Jul-20	7.5	Use-after-free issue could occur due to dangling pointer when generating a frame buffer in OpenGL ES in Snapdragon Compute, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music in APQ8009, Nicobar, QCM2150, QCS405, Saipan,	https://www.qualcomm.com/company/product-security/bulletins/july-2020-bulletin	O-QUA-SM81-190820/877

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			SDM845, SM8150, SM8250, SXR2130 **CVE ID : CVE-2020-3671**		
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	30-Jul-20	7.5	Possible buffer overflow while parsing mp4 clip with corrupted sample atoms due to improper validation of index in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables in APQ8009, APQ8017, APQ8053, APQ8096AU, APQ8098, Kamorta, MDM9206, MDM9207C, MDM9607, MSM8905, MSM8909W, MSM8917, MSM8920, MSM8937, MSM8940, MSM8953, MSM8996, MSM8996AU, MSM8998, Nicobar, QCA6574AU, QCM2150, QCS405, QCS605, QM215, Rennell, SA6155P, Saipan, SDA660, SDA845, SDM429, SDM429W, SDM439, SDM450, SDM630, SDM632, SDM636, SDM660, SDM670, SDM710, SDM845, SDX20, SM6150, SM7150, SM8150, SM8250, SXR1130, SXR2130 **CVE ID : CVE-2020-3688**	https://www.qualcomm.com/company/product-security/bulletins/july-2020-bulletin	O-QUA-SM81-190820/878
Out-of-	30-Jul-20	7.5	Out of bound write while	https://ww	O-QUA-SM81-

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
bounds Write			QoS DSCP mapping due to improper input validation for data received from association response frame 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, APQ8098, MDM9150, MDM9206, MDM9207C, MDM9607, MDM9650, MSM8905, MSM8909W, MSM8917, MSM8920, MSM8937, MSM8940, MSM8953, MSM8996AU, Nicobar, QCA6174A, QCA6574AU, QCA9377, QCA9379, QCM2150, QCN7605, QCS405, QCS605, QM215, SA6155P, Saipan, SC8180X, SDA845, SDM429, SDM429W, SDM439, SDM450, SDM630, SDM632, SDM636, SDM660, SDM845, SDX20, SDX55, SM8150, SM8250, SXR2130 **CVE ID : CVE-2020-3698**	w.qualcomm.com/company/product-security/bulletins/july-2020-bulletin	190820/879
Buffer Copy without Checking Size of Input ('Classic	30-Jul-20	7.5	Possible out of bound access while processing assoc response from host due to improper length check before copying into	https://www.qualcomm.com/company/product-security/bull	O-QUA-SM81-190820/880

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Buffer Overflow')			buffer 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, Nicobar, QCA6174A, QCA6574AU, QCA9377, QCA9379, QCM2150, QCN7605, QCS405, QCS605, QM215, SA6155P, Saipan, SC8180X, SDA845, SDM429, SDM429W, SDM439, SDM450, SDM630, SDM632, SDM636, SDM660, SDM845, SDX20, SDX55, SM6150, SM7150, SM8150, SM8250, SXR2130 **CVE ID : CVE-2020-3699**	etins/july-2020-bulletin	
Out-of-bounds Read	30-Jul-20	5	Possible out of bounds read due to a missing bounds check and could lead to local information disclosure in the wifi driver with no additional execution privileges needed in Snapdragon	https://www.qualcomm.com/company/product-security/bulletins/july-2020-	O-QUA-SM81-190820/881

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking in APQ8053, APQ8096AU, IPQ4019, IPQ8064, IPQ8074, MDM9607, MSM8909W, MSM8996AU, QCA6574AU, QCA9531, QCA9558, QCA9980, SC8180X, SDM439, SDX55, SM8150, SM8250, SXR2130 **CVE ID : CVE-2020-3700**	bulletin	
mdm9206_firmware					
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	30-Jul-20	7.5	Possible buffer overflow while parsing mp4 clip with corrupted sample atoms due to improper validation of index in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables in APQ8009, APQ8017, APQ8053, APQ8096AU, APQ8098, Kamorta, MDM9206, MDM9207C, MDM9607, MSM8905, MSM8909W, MSM8917, MSM8920, MSM8937,	https://www.qualcomm.com/company/product-security/bulletins/july-2020-bulletin	O-QUA-MDM9-190820/882

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			MSM8940, MSM8953, MSM8996, MSM8996AU, MSM8998, Nicobar, QCA6574AU, QCM2150, QCS405, QCS605, QM215, Rennell, SA6155P, Saipan, SDA660, SDA845, SDM429, SDM429W, SDM439, SDM450, SDM630, SDM632, SDM636, SDM660, SDM670, SDM710, SDM845, SDX20, SM6150, SM7150, SM8150, SM8250, SXR1130, SXR2130 **CVE ID : CVE-2020-3688**		
Out-of-bounds Write	30-Jul-20	7.5	Out of bound write while QoS DSCP mapping due to improper input validation for data received from association response frame 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, APQ8098, MDM9150, MDM9206, MDM9207C, MDM9607, MDM9650, MSM8905, MSM8909W, MSM8917, MSM8920, MSM8937, MSM8940, MSM8953, MSM8996AU, Nicobar, QCA6174A, QCA6574AU, QCA9377,	https://www.qualcomm.com/company/product-security/bulletins/july-2020-bulletin	O-QUA-MDM9-190820/883

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			QCA9379, QCM2150, QCN7605, QCS405, QCS605, QM215, SA6155P, Saipan, SC8180X, SDA845, SDM429, SDM429W, SDM439, SDM450, SDM630, SDM632, SDM636, SDM660, SDM845, SDX20, SDX55, SM8150, SM8250, SXR2130 **CVE ID : CVE-2020-3698**		
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	30-Jul-20	7.5	Possible out of bound access while processing assoc response from host due to improper length check before copying into buffer 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, Nicobar, QCA6174A, QCA6574AU, QCA9377, QCA9379, QCM2150, QCN7605, QCS405, QCS605, QM215, SA6155P, Saipan, SC8180X, SDA845,	https://www.qualcomm.com/company/product-security/bulletins/july-2020-bulletin	O-QUA-MDM9-190820/884

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			SDM429, SDM429W, SDM439, SDM450, SDM630, SDM632, SDM636, SDM660, SDM845, SDX20, SDX55, SM6150, SM7150, SM8150, SM8250, SXR2130 **CVE ID : CVE-2020-3699**		
mdm9607_firmware					
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	30-Jul-20	7.5	Possible buffer overflow while parsing mp4 clip with corrupted sample atoms due to improper validation of index in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables in APQ8009, APQ8017, APQ8053, APQ8096AU, APQ8098, Kamorta, MDM9206, MDM9207C, MDM9607, MSM8905, MSM8909W, MSM8917, MSM8920, MSM8937, MSM8940, MSM8953, MSM8996, MSM8996AU, MSM8998, Nicobar, QCA6574AU, QCM2150, QCS405, QCS605, QM215, Rennell, SA6155P, Saipan, SDA660, SDA845, SDM429, SDM429W, SDM439, SDM450, SDM630, SDM632, SDM636,	https://www.qualcomm.com/company/product-security/bulletins/july-2020-bulletin	O-QUA-MDM9-190820/885

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			SDM660, SDM670, SDM710, SDM845, SDX20, SM6150, SM7150, SM8150, SM8250, SXR1130, SXR2130 **CVE ID : CVE-2020-3688**		
Out-of-bounds Write	30-Jul-20	7.5	Out of bound write while QoS DSCP mapping due to improper input validation for data received from association response frame 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, APQ8098, MDM9150, MDM9206, MDM9207C, MDM9607, MDM9650, MSM8905, MSM8909W, MSM8917, MSM8920, MSM8937, MSM8940, MSM8953, MSM8996AU, Nicobar, QCA6174A, QCA6574AU, QCA9377, QCA9379, QCM2150, QCN7605, QCS405, QCS605, QM215, SA6155P, Saipan, SC8180X, SDA845, SDM429, SDM429W, SDM439, SDM450, SDM630, SDM632, SDM636, SDM660, SDM845, SDX20, SDX55, SM8150, SM8250,	https://www.qualcomm.com/company/product-security/bulletins/july-2020-bulletin	O-QUA-MDM9-190820/886

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			SXR2130 **CVE ID : CVE-2020-3698**		
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	30-Jul-20	7.5	Possible out of bound access while processing assoc response from host due to improper length check before copying into buffer 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, Nicobar, QCA6174A, QCA6574AU, QCA9377, QCA9379, QCM2150, QCN7605, QCS405, QCS605, QM215, SA6155P, Saipan, SC8180X, SDA845, SDM429, SDM429W, SDM439, SDM450, SDM630, SDM632, SDM636, SDM660, SDM845, SDX20, SDX55, SM6150, SM7150, SM8150, SM8250, SXR2130 **CVE ID : CVE-2020-3699**	https://www.qualcomm.com/company/product-security/bulletins/july-2020-bulletin	O-QUA-MDM9-190820/887

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Out-of-bounds Read	30-Jul-20	5	Possible out of bounds read due to a missing bounds check and could lead to local information disclosure in the wifi driver with no additional execution privileges needed in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking in APQ8053, APQ8096AU, IPQ4019, IPQ8064, IPQ8074, MDM9607, MSM8909W, MSM8996AU, QCA6574AU, QCA9531, QCA9558, QCA9980, SC8180X, SDM439, SDX55, SM8150, SM8250, SXR2130 **CVE ID : CVE-2020-3700**	https://www.qualcomm.com/company/product-security/bulletins/july-2020-bulletin	O-QUA-MDM9-190820/888
mdm9650_firmware					
Out-of-bounds Write	30-Jul-20	7.5	Out of bound write while QoS DSCP mapping due to improper input validation for data received from association response frame in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile,	https://www.qualcomm.com/company/product-security/bulletins/july-2020-bulletin	O-QUA-MDM9-190820/889

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Snapdragon Voice & Music, Snapdragon Wearables in APQ8009, APQ8017, APQ8053, APQ8096AU, APQ8098, MDM9150, MDM9206, MDM9207C, MDM9607, MDM9650, MSM8905, MSM8909W, MSM8917, MSM8920, MSM8937, MSM8940, MSM8953, MSM8996AU, Nicobar, QCA6174A, QCA6574AU, QCA9377, QCA9379, QCM2150, QCN7605, QCS405, QCS605, QM215, SA6155P, Saipan, SC8180X, SDA845, SDM429, SDM429W, SDM439, SDM450, SDM630, SDM632, SDM636, SDM660, SDM845, SDX20, SDX55, SM8150, SM8250, SXR2130 **CVE ID : CVE-2020-3698**		
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	30-Jul-20	7.5	Possible out of bound access while processing assoc response from host due to improper length check before copying into buffer 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,	https://www.qualcomm.com/company/product-security/bulletins/july-2020-bulletin	O-QUA-MDM9-190820/890

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			MDM9206, MDM9207C, MDM9607, MDM9640, MDM9650, MSM8905, MSM8909W, MSM8917, MSM8920, MSM8937, MSM8940, MSM8953, MSM8996AU, Nicobar, QCA6174A, QCA6574AU, QCA9377, QCA9379, QCM2150, QCN7605, QCS405, QCS605, QM215, SA6155P, Saipan, SC8180X, SDA845, SDM429, SDM429W, SDM439, SDM450, SDM630, SDM632, SDM636, SDM660, SDM845, SDX20, SDX55, SM6150, SM7150, SM8150, SM8250, SXR2130 **CVE ID : CVE-2020-3699**		
msm8996au_firmware					
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	30-Jul-20	7.5	Possible buffer overflow while parsing mp4 clip with corrupted sample atoms due to improper validation of index in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables in APQ8009, APQ8017, APQ8053, APQ8096AU, APQ8098, Kamorta, MDM9206, MDM9207C,	https://www.qualcomm.com/company/product-security/bulletins/july-2020-bulletin	O-QUA-MSM8-190820/891

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			MDM9607, MSM8905, MSM8909W, MSM8917, MSM8920, MSM8937, MSM8940, MSM8953, MSM8996, MSM8996AU, MSM8998, Nicobar, QCA6574AU, QCM2150, QCS405, QCS605, QM215, Rennell, SA6155P, Saipan, SDA660, SDA845, SDM429, SDM429W, SDM439, SDM450, SDM630, SDM632, SDM636, SDM660, SDM670, SDM710, SDM845, SDX20, SM6150, SM7150, SM8150, SM8250, SXR1130, SXR2130 **CVE ID : CVE-2020-3688**		
Out-of-bounds Write	30-Jul-20	7.5	Out of bound write while QoS DSCP mapping due to improper input validation for data received from association response frame 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, APQ8098, MDM9150, MDM9206, MDM9207C, MDM9607, MDM9650, MSM8905, MSM8909W, MSM8917, MSM8920, MSM8937, MSM8940,	https://www.qualcomm.com/company/product-security/bulletins/july-2020-bulletin	O-QUA-MSM8-190820/892

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			MSM8953, MSM8996AU, Nicobar, QCA6174A, QCA6574AU, QCA9377, QCA9379, QCM2150, QCN7605, QCS405, QCS605, QM215, SA6155P, Saipan, SC8180X, SDA845, SDM429, SDM429W, SDM439, SDM450, SDM630, SDM632, SDM636, SDM660, SDM845, SDX20, SDX55, SM8150, SM8250, SXR2130 **CVE ID : CVE-2020-3698**		
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	30-Jul-20	7.5	Possible out of bound access while processing assoc response from host due to improper length check before copying into buffer 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, Nicobar, QCA6174A, QCA6574AU, QCA9377, QCA9379, QCM2150, QCN7605,	https://www.qualcomm.com/company/product-security/bulletins/july-2020-bulletin	O-QUA-MSM8-190820/893

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			QCS405, QCS605, QM215, SA6155P, Saipan, SC8180X, SDA845, SDM429, SDM429W, SDM439, SDM450, SDM630, SDM632, SDM636, SDM660, SDM845, SDX20, SDX55, SM6150, SM7150, SM8150, SM8250, SXR2130 **CVE ID : CVE-2020-3699**		
Out-of-bounds Read	30-Jul-20	5	Possible out of bounds read due to a missing bounds check and could lead to local information disclosure in the wifi driver with no additional execution privileges needed in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking in APQ8053, APQ8096AU, IPQ4019, IPQ8064, IPQ8074, MDM9607, MSM8909W, MSM8996AU, QCA6574AU, QCA9531, QCA9558, QCA9980, SC8180X, SDM439, SDX55, SM8150, SM8250, SXR2130 **CVE ID : CVE-2020-3700**	https://www.qualcomm.com/company/product-security/bulletins/july-2020-bulletin	O-QUA-MSM8-190820/894
qca9531_firmware					

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Out-of-bounds Read	30-Jul-20	5	Possible out of bounds read due to a missing bounds check and could lead to local information disclosure in the wifi driver with no additional execution privileges needed in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking in APQ8053, APQ8096AU, IPQ4019, IPQ8064, IPQ8074, MDM9607, MSM8909W, MSM8996AU, QCA6574AU, QCA9531, QCA9558, QCA9980, SC8180X, SDM439, SDX55, SM8150, SM8250, SXR2130 **CVE ID : CVE-2020-3700**	https://www.qualcomm.com/company/product-security/bulletins/july-2020-bulletin	O-QUA-QCA9-190820/895
qca9980_firmware					
Out-of-bounds Read	30-Jul-20	5	Possible out of bounds read due to a missing bounds check and could lead to local information disclosure in the wifi driver with no additional execution privileges needed in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT,	https://www.qualcomm.com/company/product-security/bulletins/july-2020-bulletin	O-QUA-QCA9-190820/896

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking in APQ8053, APQ8096AU, IPQ4019, IPQ8064, IPQ8074, MDM9607, MSM8909W, MSM8996AU, QCA6574AU, QCA9531, QCA9558, QCA9980, SC8180X, SDM439, SDX55, SM8150, SM8250, SXR2130 **CVE ID : CVE-2020-3700**		
sdm429_firmware					
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	30-Jul-20	7.5	Possible buffer overflow while parsing mp4 clip with corrupted sample atoms due to improper validation of index in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables in APQ8009, APQ8017, APQ8053, APQ8096AU, APQ8098, Kamorta, MDM9206, MDM9207C, MDM9607, MSM8905, MSM8909W, MSM8917, MSM8920, MSM8937, MSM8940, MSM8953, MSM8996, MSM8996AU, MSM8998, Nicobar, QCA6574AU, QCM2150,	https://www.qualcomm.com/company/product-security/bulletins/july-2020-bulletin	O-QUA-SDM4-190820/897

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			QCS405, QCS605, QM215, Rennell, SA6155P, Saipan, SDA660, SDA845, SDM429, SDM429W, SDM439, SDM450, SDM630, SDM632, SDM636, SDM660, SDM670, SDM710, SDM845, SDX20, SM6150, SM7150, SM8150, SM8250, SXR1130, SXR2130 **CVE ID : CVE-2020-3688**		
Out-of-bounds Write	30-Jul-20	7.5	Out of bound write while QoS DSCP mapping due to improper input validation for data received from association response frame 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, APQ8098, MDM9150, MDM9206, MDM9207C, MDM9607, MDM9650, MSM8905, MSM8909W, MSM8917, MSM8920, MSM8937, MSM8940, MSM8953, MSM8996AU, Nicobar, QCA6174A, QCA6574AU, QCA9377, QCA9379, QCM2150, QCN7605, QCS405, QCS605, QM215, SA6155P, Saipan, SC8180X, SDA845,	https://www.qualcomm.com/company/product-security/bulletins/july-2020-bulletin	O-QUA-SDM4-190820/898

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			SDM429, SDM429W, SDM439, SDM450, SDM630, SDM632, SDM636, SDM660, SDM845, SDX20, SDX55, SM8150, SM8250, SXR2130 **CVE ID : CVE-2020-3698**		
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	30-Jul-20	7.5	Possible out of bound access while processing assoc response from host due to improper length check before copying into buffer 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, Nicobar, QCA6174A, QCA6574AU, QCA9377, QCA9379, QCM2150, QCN7605, QCS405, QCS605, QM215, SA6155P, Saipan, SC8180X, SDA845, SDM429, SDM429W, SDM439, SDM450, SDM630, SDM632, SDM636, SDM660,	https://www.qualcomm.com/company/product-security/bulletins/july-2020-bulletin	O-QUA-SDM4-190820/899

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			SDM845, SDX20, SDX55, SM6150, SM7150, SM8150, SM8250, SXR2130 **CVE ID : CVE-2020-3699**		
sdm632_firmware					
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	30-Jul-20	7.5	Possible buffer overflow while parsing mp4 clip with corrupted sample atoms due to improper validation of index in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables in APQ8009, APQ8017, APQ8053, APQ8096AU, APQ8098, Kamorta, MDM9206, MDM9207C, MDM9607, MSM8905, MSM8909W, MSM8917, MSM8920, MSM8937, MSM8940, MSM8953, MSM8996, MSM8996AU, MSM8998, Nicobar, QCA6574AU, QCM2150, QCS405, QCS605, QM215, Rennell, SA6155P, Saipan, SDA660, SDA845, SDM429, SDM429W, SDM439, SDM450, SDM630, SDM632, SDM636, SDM660, SDM670, SDM710, SDM845, SDX20, SM6150, SM7150, SM8150, SM8250,	https://www.qualcomm.com/company/product-security/bulletins/july-2020-bulletin	O-QUA-SDM6-190820/900

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			SXR1130, SXR2130 **CVE ID : CVE-2020-3688**		
Out-of-bounds Write	30-Jul-20	7.5	Out of bound write while QoS DSCP mapping due to improper input validation for data received from association response frame 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, APQ8098, MDM9150, MDM9206, MDM9207C, MDM9607, MDM9650, MSM8905, MSM8909W, MSM8917, MSM8920, MSM8937, MSM8940, MSM8953, MSM8996AU, Nicobar, QCA6174A, QCA6574AU, QCA9377, QCA9379, QCM2150, QCN7605, QCS405, QCS605, QM215, SA6155P, Saipan, SC8180X, SDA845, SDM429, SDM429W, SDM439, SDM450, SDM630, SDM632, SDM636, SDM660, SDM845, SDX20, SDX55, SM8150, SM8250, SXR2130 **CVE ID : CVE-2020-3698**	https://www.qualcomm.com/company/product-security/bulletins/july-2020-bulletin	O-QUA-SDM6-190820/901
Buffer Copy	30-Jul-20	7.5	Possible out of bound	https://ww	O-QUA-SDM6-

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
without Checking Size of Input ('Classic Buffer Overflow')			access while processing assoc response from host due to improper length check before copying into buffer 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, Nicobar, QCA6174A, QCA6574AU, QCA9377, QCA9379, QCM2150, QCN7605, QCS405, QCS605, QM215, SA6155P, Saipan, SC8180X, SDA845, SDM429, SDM429W, SDM439, SDM450, SDM630, SDM632, SDM636, SDM660, SDM845, SDX20, SDX55, SM6150, SM7150, SM8150, SM8250, SXR2130 **CVE ID : CVE-2020-3699**	w.qualcomm.com/company/product-security/bulletins/july-2020-bulletin	190820/902
msm8917_firmware					
Buffer Copy without	30-Jul-20	7.5	Possible buffer overflow while parsing mp4 clip	https://www.qualcomm.	O-QUA-MSM8-

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Checking Size of Input ('Classic Buffer Overflow')			with corrupted sample atoms due to improper validation of index in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables in APQ8009, APQ8017, APQ8053, APQ8096AU, APQ8098, Kamorta, MDM9206, MDM9207C, MDM9607, MSM8905, MSM8909W, MSM8917, MSM8920, MSM8937, MSM8940, MSM8953, MSM8996, MSM8996AU, MSM8998, Nicobar, QCA6574AU, QCM2150, QCS405, QCS605, QM215, Rennell, SA6155P, Saipan, SDA660, SDA845, SDM429, SDM429W, SDM439, SDM450, SDM630, SDM632, SDM636, SDM660, SDM670, SDM710, SDM845, SDX20, SM6150, SM7150, SM8150, SM8250, SXR1130, SXR2130 **CVE ID : CVE-2020-3688**	com/company/product-security/bulletins/july-2020-bulletin	190820/903
Out-of-bounds Write	30-Jul-20	7.5	Out of bound write while QoS DSCP mapping due to improper input validation for data received from association response frame in Snapdragon Auto, Snapdragon Compute,	https://www.qualcomm.com/company/product-security/bulletins/july-2020-	O-QUA-MSM8-190820/904

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables in APQ8009, APQ8017, APQ8053, APQ8096AU, APQ8098, MDM9150, MDM9206, MDM9207C, MDM9607, MDM9650, MSM8905, MSM8909W, MSM8917, MSM8920, MSM8937, MSM8940, MSM8953, MSM8996AU, Nicobar, QCA6174A, QCA6574AU, QCA9377, QCA9379, QCM2150, QCN7605, QCS405, QCS605, QM215, SA6155P, Saipan, SC8180X, SDA845, SDM429, SDM429W, SDM439, SDM450, SDM630, SDM632, SDM636, SDM660, SDM845, SDX20, SDX55, SM8150, SM8250, SXR2130 **CVE ID : CVE-2020-3698**	bulletin	
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	30-Jul-20	7.5	Possible out of bound access while processing assoc response from host due to improper length check before copying into buffer in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial	https://www.qualcomm.com/company/product-security/bulletins/july-2020-bulletin	O-QUA-MSM8-190820/905

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			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, Nicobar, QCA6174A, QCA6574AU, QCA9377, QCA9379, QCM2150, QCN7605, QCS405, QCS605, QM215, SA6155P, Saipan, SC8180X, SDA845, SDM429, SDM429W, SDM439, SDM450, SDM630, SDM632, SDM636, SDM660, SDM845, SDX20, SDX55, SM6150, SM7150, SM8150, SM8250, SXR2130 **CVE ID : CVE-2020-3699**		
msm8920_firmware					
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	30-Jul-20	7.5	Possible buffer overflow while parsing mp4 clip with corrupted sample atoms due to improper validation of index in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music,	https://www.qualcomm.com/company/product-security/bulletins/july-2020-bulletin	O-QUA-MSM8-190820/906

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Snapdragon Wearables in APQ8009, APQ8017, APQ8053, APQ8096AU, APQ8098, Kamorta, MDM9206, MDM9207C, MDM9607, MSM8905, MSM8909W, MSM8917, MSM8920, MSM8937, MSM8940, MSM8953, MSM8996, MSM8996AU, MSM8998, Nicobar, QCA6574AU, QCM2150, QCS405, QCS605, QM215, Rennell, SA6155P, Saipan, SDA660, SDA845, SDM429, SDM429W, SDM439, SDM450, SDM630, SDM632, SDM636, SDM660, SDM670, SDM710, SDM845, SDX20, SM6150, SM7150, SM8150, SM8250, SXR1130, SXR2130 **CVE ID : CVE-2020-3688**		
Out-of-bounds Write	30-Jul-20	7.5	Out of bound write while QoS DSCP mapping due to improper input validation for data received from association response frame 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, APQ8098, MDM9150,	https://www.qualcomm.com/company/product-security/bulletins/july-2020-bulletin	O-QUA-MSM8-190820/907

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			MDM9206, MDM9207C, MDM9607, MDM9650, MSM8905, MSM8909W, MSM8917, MSM8920, MSM8937, MSM8940, MSM8953, MSM8996AU, Nicobar, QCA6174A, QCA6574AU, QCA9377, QCA9379, QCM2150, QCN7605, QCS405, QCS605, QM215, SA6155P, Saipan, SC8180X, SDA845, SDM429, SDM429W, SDM439, SDM450, SDM630, SDM632, SDM636, SDM660, SDM845, SDX20, SDX55, SM8150, SM8250, SXR2130 **CVE ID : CVE-2020-3698**		
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	30-Jul-20	7.5	Possible out of bound access while processing assoc response from host due to improper length check before copying into buffer 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,	https://www.qualcomm.com/company/product-security/bulletins/july-2020-bulletin	O-QUA-MSM8-190820/908

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			MSM8940, MSM8953, MSM8996AU, Nicobar, QCA6174A, QCA6574AU, QCA9377, QCA9379, QCM2150, QCN7605, QCS405, QCS605, QM215, SA6155P, Saipan, SC8180X, SDA845, SDM429, SDM429W, SDM439, SDM450, SDM630, SDM632, SDM636, SDM660, SDM845, SDX20, SDX55, SM6150, SM7150, SM8150, SM8250, SXR2130 **CVE ID : CVE-2020-3699**		
msm8937_firmware					
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	30-Jul-20	7.5	Possible buffer overflow while parsing mp4 clip with corrupted sample atoms due to improper validation of index in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables in APQ8009, APQ8017, APQ8053, APQ8096AU, APQ8098, Kamorta, MDM9206, MDM9207C, MDM9607, MSM8905, MSM8909W, MSM8917, MSM8920, MSM8937, MSM8940, MSM8953, MSM8996, MSM8996AU,	https://www.qualcomm.com/company/product-security/bulletins/july-2020-bulletin	O-QUA-MSM8-190820/909

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			MSM8998, Nicobar, QCA6574AU, QCM2150, QCS405, QCS605, QM215, Rennell, SA6155P, Saipan, SDA660, SDA845, SDM429, SDM429W, SDM439, SDM450, SDM630, SDM632, SDM636, SDM660, SDM670, SDM710, SDM845, SDX20, SM6150, SM7150, SM8150, SM8250, SXR1130, SXR2130 **CVE ID : CVE-2020-3688**		
Out-of-bounds Write	30-Jul-20	7.5	Out of bound write while QoS DSCP mapping due to improper input validation for data received from association response frame 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, APQ8098, MDM9150, MDM9206, MDM9207C, MDM9607, MDM9650, MSM8905, MSM8909W, MSM8917, MSM8920, MSM8937, MSM8940, MSM8953, MSM8996AU, Nicobar, QCA6174A, QCA6574AU, QCA9377, QCA9379, QCM2150, QCN7605, QCS405,	https://www.qualcomm.com/company/product-security/bulletins/july-2020-bulletin	O-QUA-MSM8-190820/910

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			QCS605, QM215, SA6155P, Saipan, SC8180X, SDA845, SDM429, SDM429W, SDM439, SDM450, SDM630, SDM632, SDM636, SDM660, SDM845, SDX20, SDX55, SM8150, SM8250, SXR2130 **CVE ID : CVE-2020-3698**		
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	30-Jul-20	7.5	Possible out of bound access while processing assoc response from host due to improper length check before copying into buffer 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, Nicobar, QCA6174A, QCA6574AU, QCA9377, QCA9379, QCM2150, QCN7605, QCS405, QCS605, QM215, SA6155P, Saipan, SC8180X, SDA845, SDM429, SDM429W, SDM439, SDM450,	https://www.qualcomm.com/company/product-security/bulletins/july-2020-bulletin	O-QUA-MSM8-190820/911

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			SDM630, SDM632, SDM636, SDM660, SDM845, SDX20, SDX55, SM6150, SM7150, SM8150, SM8250, SXR2130 **CVE ID : CVE-2020-3699**		
msm8940_firmware					
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	30-Jul-20	7.5	Possible buffer overflow while parsing mp4 clip with corrupted sample atoms due to improper validation of index in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables in APQ8009, APQ8017, APQ8053, APQ8096AU, APQ8098, Kamorta, MDM9206, MDM9207C, MDM9607, MSM8905, MSM8909W, MSM8917, MSM8920, MSM8937, MSM8940, MSM8953, MSM8996, MSM8996AU, MSM8998, Nicobar, QCA6574AU, QCM2150, QCS405, QCS605, QM215, Rennell, SA6155P, Saipan, SDA660, SDA845, SDM429, SDM429W, SDM439, SDM450, SDM630, SDM632, SDM636, SDM660, SDM670, SDM710, SDM845, SDX20,	https://www.qualcomm.com/company/product-security/bulletins/july-2020-bulletin	O-QUA-MSM8-190820/912

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			SM6150, SM7150, SM8150, SM8250, SXR1130, SXR2130 **CVE ID : CVE-2020-3688**		
Out-of-bounds Write	30-Jul-20	7.5	Out of bound write while QoS DSCP mapping due to improper input validation for data received from association response frame 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, APQ8098, MDM9150, MDM9206, MDM9207C, MDM9607, MDM9650, MSM8905, MSM8909W, MSM8917, MSM8920, MSM8937, MSM8940, MSM8953, MSM8996AU, Nicobar, QCA6174A, QCA6574AU, QCA9377, QCA9379, QCM2150, QCN7605, QCS405, QCS605, QM215, SA6155P, Saipan, SC8180X, SDA845, SDM429, SDM429W, SDM439, SDM450, SDM630, SDM632, SDM636, SDM660, SDM845, SDX20, SDX55, SM8150, SM8250, SXR2130	https://www.qualcomm.com/company/product-security/bulletins/july-2020-bulletin	O-QUA-MSM8-190820/913

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2020-3698		
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	30-Jul-20	7.5	Possible out of bound access while processing assoc response from host due to improper length check before copying into buffer 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, Nicobar, QCA6174A, QCA6574AU, QCA9377, QCA9379, QCM2150, QCN7605, QCS405, QCS605, QM215, SA6155P, Saipan, SC8180X, SDA845, SDM429, SDM429W, SDM439, SDM450, SDM630, SDM632, SDM636, SDM660, SDM845, SDX20, SDX55, SM6150, SM7150, SM8150, SM8250, SXR2130 **CVE ID : CVE-2020-3699**	https://www.qualcomm.com/company/product-security/bulletins/july-2020-bulletin	O-QUA-MSM8-190820/914
msm8996_firmware					

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	30-Jul-20	7.5	Possible buffer overflow while parsing mp4 clip with corrupted sample atoms due to improper validation of index in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables in APQ8009, APQ8017, APQ8053, APQ8096AU, APQ8098, Kamorta, MDM9206, MDM9207C, MDM9607, MSM8905, MSM8909W, MSM8917, MSM8920, MSM8937, MSM8940, MSM8953, MSM8996, MSM8996AU, MSM8998, Nicobar, QCA6574AU, QCM2150, QCS405, QCS605, QM215, Rennell, SA6155P, Saipan, SDA660, SDA845, SDM429, SDM429W, SDM439, SDM450, SDM630, SDM632, SDM636, SDM660, SDM670, SDM710, SDM845, SDX20, SM6150, SM7150, SM8150, SM8250, SXR1130, SXR2130 **CVE ID : CVE-2020-3688**	https://www.qualcomm.com/company/product-security/bulletins/july-2020-bulletin	O-QUA-MSM8-190820/915
sdm450_firmware					
Buffer Copy without Checking	30-Jul-20	7.5	Possible buffer overflow while parsing mp4 clip with corrupted sample	https://www.qualcomm.com/compan	O-QUA-SDM4-190820/916

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Size of Input ('Classic Buffer Overflow')			atoms due to improper validation of index in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables in APQ8009, APQ8017, APQ8053, APQ8096AU, APQ8098, Kamorta, MDM9206, MDM9207C, MDM9607, MSM8905, MSM8909W, MSM8917, MSM8920, MSM8937, MSM8940, MSM8953, MSM8996, MSM8996AU, MSM8998, Nicobar, QCA6574AU, QCM2150, QCS405, QCS605, QM215, Rennell, SA6155P, Saipan, SDA660, SDA845, SDM429, SDM429W, SDM439, SDM450, SDM630, SDM632, SDM636, SDM660, SDM670, SDM710, SDM845, SDX20, SM6150, SM7150, SM8150, SM8250, SXR1130, SXR2130 **CVE ID : CVE-2020-3688**	y/product-security/bulletins/july-2020-bulletin	
Out-of-bounds Write	30-Jul-20	7.5	Out of bound write while QoS DSCP mapping due to improper input validation for data received from association response frame in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer	https://www.qualcomm.com/company/product-security/bulletins/july-2020-	O-QUA-SDM4-190820/917

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, APQ8098, MDM9150, MDM9206, MDM9207C, MDM9607, MDM9650, MSM8905, MSM8909W, MSM8917, MSM8920, MSM8937, MSM8940, MSM8953, MSM8996AU, Nicobar, QCA6174A, QCA6574AU, QCA9377, QCA9379, QCM2150, QCN7605, QCS405, QCS605, QM215, SA6155P, Saipan, SC8180X, SDA845, SDM429, SDM429W, SDM439, SDM450, SDM630, SDM632, SDM636, SDM660, SDM845, SDX20, SDX55, SM8150, SM8250, SXR2130 **CVE ID : CVE-2020-3698**	bulletin	
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	30-Jul-20	7.5	Possible out of bound access while processing assoc response from host due to improper length check before copying into buffer in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile,	https://www.qualcomm.com/company/product-security/bulletins/july-2020-bulletin	O-QUA-SDM4-190820/918

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Snapdragon Voice & Music, Snapdragon Wearables in APQ8009, APQ8017, APQ8053, APQ8096AU, MDM9206, MDM9207C, MDM9607, MDM9640, MDM9650, MSM8905, MSM8909W, MSM8917, MSM8920, MSM8937, MSM8940, MSM8953, MSM8996AU, Nicobar, QCA6174A, QCA6574AU, QCA9377, QCA9379, QCM2150, QCN7605, QCS405, QCS605, QM215, SA6155P, Saipan, SC8180X, SDA845, SDM429, SDM429W, SDM439, SDM450, SDM630, SDM632, SDM636, SDM660, SDM845, SDX20, SDX55, SM6150, SM7150, SM8150, SM8250, SXR2130 **CVE ID : CVE-2020-3699**		
sm8250_firmware					
Use After Free	30-Jul-20	7.5	Use-after-free issue could occur due to dangling pointer when generating a frame buffer in OpenGL ES in Snapdragon Compute, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music in APQ8009, Nicobar, QCM2150, QCS405, Saipan, SDM845, SM8150, SM8250, SXR2130	https://www.qualcomm.com/company/product-security/bulletins/july-2020-bulletin	O-QUA-SM82-190820/919

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2020-3671		
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	30-Jul-20	7.5	Possible buffer overflow while parsing mp4 clip with corrupted sample atoms due to improper validation of index in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables in APQ8009, APQ8017, APQ8053, APQ8096AU, APQ8098, Kamorta, MDM9206, MDM9207C, MDM9607, MSM8905, MSM8909W, MSM8917, MSM8920, MSM8937, MSM8940, MSM8953, MSM8996, MSM8996AU, MSM8998, Nicobar, QCA6574AU, QCM2150, QCS405, QCS605, QM215, Rennell, SA6155P, Saipan, SDA660, SDA845, SDM429, SDM429W, SDM439, SDM450, SDM630, SDM632, SDM636, SDM660, SDM670, SDM710, SDM845, SDX20, SM6150, SM7150, SM8150, SM8250, SXR1130, SXR2130 **CVE ID : CVE-2020-3688**	https://www.qualcomm.com/company/product-security/bulletins/july-2020-bulletin	O-QUA-SM82-190820/920
Out-of-bounds Write	30-Jul-20	7.5	Out of bound write while QoS DSCP mapping due to improper input validation	https://www.qualcomm.com/compan	O-QUA-SM82-190820/921

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			for data received from association response frame 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, APQ8098, MDM9150, MDM9206, MDM9207C, MDM9607, MDM9650, MSM8905, MSM8909W, MSM8917, MSM8920, MSM8937, MSM8940, MSM8953, MSM8996AU, Nicobar, QCA6174A, QCA6574AU, QCA9377, QCA9379, QCM2150, QCN7605, QCS405, QCS605, QM215, SA6155P, Saipan, SC8180X, SDA845, SDM429, SDM429W, SDM439, SDM450, SDM630, SDM632, SDM636, SDM660, SDM845, SDX20, SDX55, SM8150, SM8250, SXR2130 **CVE ID : CVE-2020-3698**	y/product-security/bulletins/july-2020-bulletin	
Buffer Copy without Checking Size of Input ('Classic Buffer	30-Jul-20	7.5	Possible out of bound access while processing assoc response from host due to improper length check before copying into buffer in Snapdragon Auto, Snapdragon Compute,	https://www.qualcomm.com/company/product-security/bulletins/july-2020-	O-QUA-SM82-190820/922

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Overflow')			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, Nicobar, QCA6174A, QCA6574AU, QCA9377, QCA9379, QCM2150, QCN7605, QCS405, QCS605, QM215, SA6155P, Saipan, SC8180X, SDA845, SDM429, SDM429W, SDM439, SDM450, SDM630, SDM632, SDM636, SDM660, SDM845, SDX20, SDX55, SM6150, SM7150, SM8150, SM8250, SXR2130 **CVE ID : CVE-2020-3699**	bulletin	
Out-of-bounds Read	30-Jul-20	5	Possible out of bounds read due to a missing bounds check and could lead to local information disclosure in the wifi driver with no additional execution privileges needed in Snapdragon Auto, Snapdragon Compute, Snapdragon	https://www.qualcomm.com/company/product-security/bulletins/july-2020-bulletin	O-QUA-SM82-190820/923

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Connectivity, Snapdragon Consumer IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking in APQ8053, APQ8096AU, IPQ4019, IPQ8064, IPQ8074, MDM9607, MSM8909W, MSM8996AU, QCA6574AU, QCA9531, QCA9558, QCA9980, SC8180X, SDM439, SDX55, SM8150, SM8250, SXR2130 **CVE ID : CVE-2020-3700**		
Use After Free	30-Jul-20	4.6	Use after free issue while processing error notification from camx driver due to not properly releasing the sequence data in Snapdragon Mobile in Saipan, SM8250, SXR2130 **CVE ID : CVE-2020-3701**	https://www.qualcomm.com/company/product-security/bulletins/july-2020-bulletin	O-QUA-SM82-190820/924
sxr2130_firmware					
Use After Free	30-Jul-20	7.5	Use-after-free issue could occur due to dangling pointer when generating a frame buffer in OpenGL ES in Snapdragon Compute, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music in APQ8009, Nicobar, QCM2150, QCS405, Saipan, SDM845, SM8150,	https://www.qualcomm.com/company/product-security/bulletins/july-2020-bulletin	O-QUA-SXR2-190820/925

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			SM8250, SXR2130 **CVE ID : CVE-2020-3671**		
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	30-Jul-20	7.5	Possible buffer overflow while parsing mp4 clip with corrupted sample atoms due to improper validation of index in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables in APQ8009, APQ8017, APQ8053, APQ8096AU, APQ8098, Kamorta, MDM9206, MDM9207C, MDM9607, MSM8905, MSM8909W, MSM8917, MSM8920, MSM8937, MSM8940, MSM8953, MSM8996, MSM8996AU, MSM8998, Nicobar, QCA6574AU, QCM2150, QCS405, QCS605, QM215, Rennell, SA6155P, Saipan, SDA660, SDA845, SDM429, SDM429W, SDM439, SDM450, SDM630, SDM632, SDM636, SDM660, SDM670, SDM710, SDM845, SDX20, SM6150, SM7150, SM8150, SM8250, SXR1130, SXR2130 **CVE ID : CVE-2020-3688**	https://www.qualcomm.com/company/product-security/bulletins/july-2020-bulletin	O-QUA-SXR2-190820/926
Out-of-bounds	30-Jul-20	7.5	Out of bound write while QoS DSCP mapping due to	https://www.qualcomm.	O-QUA-SXR2-190820/927

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Write			improper input validation for data received from association response frame 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, APQ8098, MDM9150, MDM9206, MDM9207C, MDM9607, MDM9650, MSM8905, MSM8909W, MSM8917, MSM8920, MSM8937, MSM8940, MSM8953, MSM8996AU, Nicobar, QCA6174A, QCA6574AU, QCA9377, QCA9379, QCM2150, QCN7605, QCS405, QCS605, QM215, SA6155P, Saipan, SC8180X, SDA845, SDM429, SDM429W, SDM439, SDM450, SDM630, SDM632, SDM636, SDM660, SDM845, SDX20, SDX55, SM8150, SM8250, SXR2130 **CVE ID : CVE-2020-3698**	com/company/product-security/bulletins/july-2020-bulletin	
Buffer Copy without Checking Size of Input ('Classic Buffer	30-Jul-20	7.5	Possible out of bound access while processing assoc response from host due to improper length check before copying into buffer in Snapdragon Auto,	https://www.qualcomm.com/company/product-security/bulletins/july-	O-QUA-SXR2-190820/928

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Overflow')			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, Nicobar, QCA6174A, QCA6574AU, QCA9377, QCA9379, QCM2150, QCN7605, QCS405, QCS605, QM215, SA6155P, Saipan, SC8180X, SDA845, SDM429, SDM429W, SDM439, SDM450, SDM630, SDM632, SDM636, SDM660, SDM845, SDX20, SDX55, SM6150, SM7150, SM8150, SM8250, SXR2130 **CVE ID : CVE-2020-3699**	2020-bulletin	
Out-of-bounds Read	30-Jul-20	5	Possible out of bounds read due to a missing bounds check and could lead to local information disclosure in the wifi driver with no additional execution privileges needed in Snapdragon Auto, Snapdragon	https://www.qualcomm.com/company/product-security/bulletins/july-2020-bulletin	O-QUA-SXR2-190820/929

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking in APQ8053, APQ8096AU, IPQ4019, IPQ8064, IPQ8074, MDM9607, MSM8909W, MSM8996AU, QCA6574AU, QCA9531, QCA9558, QCA9980, SC8180X, SDM439, SDX55, SM8150, SM8250, SXR2130 **CVE ID : CVE-2020-3700**		
Use After Free	30-Jul-20	4.6	Use after free issue while processing error notification from camx driver due to not properly releasing the sequence data in Snapdragon Mobile in Saipan, SM8250, SXR2130 **CVE ID : CVE-2020-3701**	https://www.qualcomm.com/company/product-security/bulletins/july-2020-bulletin	O-QUA-SXR2-190820/930
sa6155p_firmware					
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	30-Jul-20	7.5	Possible buffer overflow while parsing mp4 clip with corrupted sample atoms due to improper validation of index in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music,	https://www.qualcomm.com/company/product-security/bulletins/july-2020-bulletin	O-QUA-SA61-190820/931

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Snapdragon Wearables in APQ8009, APQ8017, APQ8053, APQ8096AU, APQ8098, Kamorta, MDM9206, MDM9207C, MDM9607, MSM8905, MSM8909W, MSM8917, MSM8920, MSM8937, MSM8940, MSM8953, MSM8996, MSM8996AU, MSM8998, Nicobar, QCA6574AU, QCM2150, QCS405, QCS605, QM215, Rennell, SA6155P, Saipan, SDA660, SDA845, SDM429, SDM429W, SDM439, SDM450, SDM630, SDM632, SDM636, SDM660, SDM670, SDM710, SDM845, SDX20, SM6150, SM7150, SM8150, SM8250, SXR1130, SXR2130 **CVE ID : CVE-2020-3688**		
Out-of-bounds Write	30-Jul-20	7.5	Out of bound write while QoS DSCP mapping due to improper input validation for data received from association response frame 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, APQ8098, MDM9150,	https://www.qualcomm.com/company/product-security/bulletins/july-2020-bulletin	O-QUA-SA61-190820/932

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			MDM9206, MDM9207C, MDM9607, MDM9650, MSM8905, MSM8909W, MSM8917, MSM8920, MSM8937, MSM8940, MSM8953, MSM8996AU, Nicobar, QCA6174A, QCA6574AU, QCA9377, QCA9379, QCM2150, QCN7605, QCS405, QCS605, QM215, SA6155P, Saipan, SC8180X, SDA845, SDM429, SDM429W, SDM439, SDM450, SDM630, SDM632, SDM636, SDM660, SDM845, SDX20, SDX55, SM8150, SM8250, SXR2130 **CVE ID : CVE-2020-3698**		
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	30-Jul-20	7.5	Possible out of bound access while processing assoc response from host due to improper length check before copying into buffer 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,	https://www.qualcomm.com/company/product-security/bulletins/july-2020-bulletin	O-QUA-SA61-190820/933

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			MSM8940, MSM8953, MSM8996AU, Nicobar, QCA6174A, QCA6574AU, QCA9377, QCA9379, QCM2150, QCN7605, QCS405, QCS605, QM215, SA6155P, Saipan, SC8180X, SDA845, SDM429, SDM429W, SDM439, SDM450, SDM630, SDM632, SDM636, SDM660, SDM845, SDX20, SDX55, SM6150, SM7150, SM8150, SM8250, SXR2130 **CVE ID : CVE-2020-3699**		
sc8180x_firmware					
Out-of-bounds Write	30-Jul-20	7.5	Out of bound write while QoS DSCP mapping due to improper input validation for data received from association response frame 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, APQ8098, MDM9150, MDM9206, MDM9207C, MDM9607, MDM9650, MSM8905, MSM8909W, MSM8917, MSM8920, MSM8937, MSM8940,	https://www.qualcomm.com/company/product-security/bulletins/july-2020-bulletin	O-QUA-SC81-190820/934

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			MSM8953, MSM8996AU, Nicobar, QCA6174A, QCA6574AU, QCA9377, QCA9379, QCM2150, QCN7605, QCS405, QCS605, QM215, SA6155P, Saipan, SC8180X, SDA845, SDM429, SDM429W, SDM439, SDM450, SDM630, SDM632, SDM636, SDM660, SDM845, SDX20, SDX55, SM8150, SM8250, SXR2130 **CVE ID : CVE-2020-3698**		
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	30-Jul-20	7.5	Possible out of bound access while processing assoc response from host due to improper length check before copying into buffer 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, Nicobar, QCA6174A, QCA6574AU, QCA9377, QCA9379, QCM2150, QCN7605,	https://www.qualcomm.com/company/product-security/bulletins/july-2020-bulletin	O-QUA-SC81-190820/935

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			QCS405, QCS605, QM215, SA6155P, Saipan, SC8180X, SDA845, SDM429, SDM429W, SDM439, SDM450, SDM630, SDM632, SDM636, SDM660, SDM845, SDX20, SDX55, SM6150, SM7150, SM8150, SM8250, SXR2130 **CVE ID : CVE-2020-3699**		
Out-of-bounds Read	30-Jul-20	5	Possible out of bounds read due to a missing bounds check and could lead to local information disclosure in the wifi driver with no additional execution privileges needed in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking in APQ8053, APQ8096AU, IPQ4019, IPQ8064, IPQ8074, MDM9607, MSM8909W, MSM8996AU, QCA6574AU, QCA9531, QCA9558, QCA9980, SC8180X, SDM439, SDX55, SM8150, SM8250, SXR2130 **CVE ID : CVE-2020-3700**	https://www.qualcomm.com/company/product-security/bulletins/july-2020-bulletin	O-QUA-SC81-190820/936
qcm2150_firmware					

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Use After Free	30-Jul-20	7.5	Use-after-free issue could occur due to dangling pointer when generating a frame buffer in OpenGL ES in Snapdragon Compute, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music in APQ8009, Nicobar, QCM2150, QCS405, Saipan, SDM845, SM8150, SM8250, SXR2130 **CVE ID : CVE-2020-3671**	https://www.qualcomm.com/company/product-security/bulletins/july-2020-bulletin	O-QUA-QCM2-190820/937
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	30-Jul-20	7.5	Possible buffer overflow while parsing mp4 clip with corrupted sample atoms due to improper validation of index in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables in APQ8009, APQ8017, APQ8053, APQ8096AU, APQ8098, Kamorta, MDM9206, MDM9207C, MDM9607, MSM8905, MSM8909W, MSM8917, MSM8920, MSM8937, MSM8940, MSM8953, MSM8996, MSM8996AU, MSM8998, Nicobar, QCA6574AU, QCM2150, QCS405, QCS605, QM215, Rennell, SA6155P, Saipan, SDA660, SDA845, SDM429,	https://www.qualcomm.com/company/product-security/bulletins/july-2020-bulletin	O-QUA-QCM2-190820/938

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			SDM429W, SDM439, SDM450, SDM630, SDM632, SDM636, SDM660, SDM670, SDM710, SDM845, SDX20, SM6150, SM7150, SM8150, SM8250, SXR1130, SXR2130 **CVE ID : CVE-2020-3688**		
Out-of-bounds Write	30-Jul-20	7.5	Out of bound write while QoS DSCP mapping due to improper input validation for data received from association response frame 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, APQ8098, MDM9150, MDM9206, MDM9207C, MDM9607, MDM9650, MSM8905, MSM8909W, MSM8917, MSM8920, MSM8937, MSM8940, MSM8953, MSM8996AU, Nicobar, QCA6174A, QCA6574AU, QCA9377, QCA9379, QCM2150, QCN7605, QCS405, QCS605, QM215, SA6155P, Saipan, SC8180X, SDA845, SDM429, SDM429W, SDM439, SDM450, SDM630, SDM632,	https://www.qualcomm.com/company/product-security/bulletins/july-2020-bulletin	O-QUA-QCM2-190820/939

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			SDM636, SDM660, SDM845, SDX20, SDX55, SM8150, SM8250, SXR2130 **CVE ID : CVE-2020-3698**		
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	30-Jul-20	7.5	Possible out of bound access while processing assoc response from host due to improper length check before copying into buffer 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, Nicobar, QCA6174A, QCA6574AU, QCA9377, QCA9379, QCM2150, QCN7605, QCS405, QCS605, QM215, SA6155P, Saipan, SC8180X, SDA845, SDM429, SDM429W, SDM439, SDM450, SDM630, SDM632, SDM636, SDM660, SDM845, SDX20, SDX55, SM6150, SM7150, SM8150, SM8250,	https://www.qualcomm.com/company/product-security/bulletins/july-2020-bulletin	O-QUA-QCM2-190820/940

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			SXR2130 **CVE ID : CVE-2020-3699**		
sdx55_firmware					
Out-of-bounds Write	30-Jul-20	7.5	Out of bound write while QoS DSCP mapping due to improper input validation for data received from association response frame 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, APQ8098, MDM9150, MDM9206, MDM9207C, MDM9607, MDM9650, MSM8905, MSM8909W, MSM8917, MSM8920, MSM8937, MSM8940, MSM8953, MSM8996AU, Nicobar, QCA6174A, QCA6574AU, QCA9377, QCA9379, QCM2150, QCN7605, QCS405, QCS605, QM215, SA6155P, Saipan, SC8180X, SDA845, SDM429, SDM429W, SDM439, SDM450, SDM630, SDM632, SDM636, SDM660, SDM845, SDX20, SDX55, SM8150, SM8250, SXR2130 **CVE ID : CVE-2020-3698**	https://www.qualcomm.com/company/product-security/bulletins/july-2020-bulletin	O-QUA-SDX5-190820/941

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	30-Jul-20	7.5	Possible out of bound access while processing assoc response from host due to improper length check before copying into buffer 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, Nicobar, QCA6174A, QCA6574AU, QCA9377, QCA9379, QCM2150, QCN7605, QCS405, QCS605, QM215, SA6155P, Saipan, SC8180X, SDA845, SDM429, SDM429W, SDM439, SDM450, SDM630, SDM632, SDM636, SDM660, SDM845, SDX20, SDX55, SM6150, SM7150, SM8150, SM8250, SXR2130 **CVE ID : CVE-2020-3699**	https://www.qualcomm.com/company/product-security/bulletins/july-2020-bulletin	O-QUA-SDX5-190820/942
Out-of-bounds Read	30-Jul-20	5	Possible out of bounds read due to a missing bounds check and could	https://www.qualcomm.com/compan	O-QUA-SDX5-190820/943

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			lead to local information disclosure in the wifi driver with no additional execution privileges needed in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking in APQ8053, APQ8096AU, IPQ4019, IPQ8064, IPQ8074, MDM9607, MSM8909W, MSM8996AU, QCA6574AU, QCA9531, QCA9558, QCA9980, SC8180X, SDM439, SDX55, SM8150, SM8250, SXR2130 **CVE ID : CVE-2020-3700**	y/product-security/bulletins/july-2020-bulletin	
sda660_firmware					
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	30-Jul-20	7.5	Possible buffer overflow while parsing mp4 clip with corrupted sample atoms due to improper validation of index in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables in APQ8009, APQ8017, APQ8053, APQ8096AU,	https://www.qualcomm.com/company/product-security/bulletins/july-2020-bulletin	O-QUA-SDA6-190820/944

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			APQ8098, Kamorta, MDM9206, MDM9207C, MDM9607, MSM8905, MSM8909W, MSM8917, MSM8920, MSM8937, MSM8940, MSM8953, MSM8996, MSM8996AU, MSM8998, Nicobar, QCA6574AU, QCM2150, QCS405, QCS605, QM215, Rennell, SA6155P, Saipan, SDA660, SDA845, SDM429, SDM429W, SDM439, SDM450, SDM630, SDM632, SDM636, SDM660, SDM670, SDM710, SDM845, SDX20, SM6150, SM7150, SM8150, SM8250, SXR1130, SXR2130 **CVE ID : CVE-2020-3688**		
sdm439_firmware					
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	30-Jul-20	7.5	Possible buffer overflow while parsing mp4 clip with corrupted sample atoms due to improper validation of index in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables in APQ8009, APQ8017, APQ8053, APQ8096AU, APQ8098, Kamorta, MDM9206, MDM9207C, MDM9607, MSM8905,	https://www.qualcomm.com/company/product-security/bulletins/july-2020-bulletin	O-QUA-SDM4-190820/945

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			MSM8909W, MSM8917, MSM8920, MSM8937, MSM8940, MSM8953, MSM8996, MSM8996AU, MSM8998, Nicobar, QCA6574AU, QCM2150, QCS405, QCS605, QM215, Rennell, SA6155P, Saipan, SDA660, SDA845, SDM429, SDM429W, SDM439, SDM450, SDM630, SDM632, SDM636, SDM660, SDM670, SDM710, SDM845, SDX20, SM6150, SM7150, SM8150, SM8250, SXR1130, SXR2130 **CVE ID : CVE-2020-3688**		
Out-of-bounds Write	30-Jul-20	7.5	Out of bound write while QoS DSCP mapping due to improper input validation for data received from association response frame 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, APQ8098, MDM9150, MDM9206, MDM9207C, MDM9607, MDM9650, MSM8905, MSM8909W, MSM8917, MSM8920, MSM8937, MSM8940, MSM8953, MSM8996AU,	https://www.qualcomm.com/company/product-security/bulletins/july-2020-bulletin	O-QUA-SDM4-190820/946

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Nicobar, QCA6174A, QCA6574AU, QCA9377, QCA9379, QCM2150, QCN7605, QCS405, QCS605, QM215, SA6155P, Saipan, SC8180X, SDA845, SDM429, SDM429W, SDM439, SDM450, SDM630, SDM632, SDM636, SDM660, SDM845, SDX20, SDX55, SM8150, SM8250, SXR2130 **CVE ID : CVE-2020-3698**		
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	30-Jul-20	7.5	Possible out of bound access while processing assoc response from host due to improper length check before copying into buffer 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, Nicobar, QCA6174A, QCA6574AU, QCA9377, QCA9379, QCM2150, QCN7605, QCS405, QCS605, QM215,	https://www.qualcomm.com/company/product-security/bulletins/july-2020-bulletin	O-QUA-SDM4-190820/947

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			SA6155P, Saipan, SC8180X, SDA845, SDM429, SDM429W, SDM439, SDM450, SDM630, SDM632, SDM636, SDM660, SDM845, SDX20, SDX55, SM6150, SM7150, SM8150, SM8250, SXR2130 **CVE ID : CVE-2020-3699**		
Out-of-bounds Read	30-Jul-20	5	Possible out of bounds read due to a missing bounds check and could lead to local information disclosure in the wifi driver with no additional execution privileges needed in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking in APQ8053, APQ8096AU, IPQ4019, IPQ8064, IPQ8074, MDM9607, MSM8909W, MSM8996AU, QCA6574AU, QCA9531, QCA9558, QCA9980, SC8180X, SDM439, SDX55, SM8150, SM8250, SXR2130 **CVE ID : CVE-2020-3700**	https://www.qualcomm.com/company/product-security/bulletins/july-2020-bulletin	O-QUA-SDM4-190820/948
sdm630_firmware					

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	30-Jul-20	7.5	Possible buffer overflow while parsing mp4 clip with corrupted sample atoms due to improper validation of index in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables in APQ8009, APQ8017, APQ8053, APQ8096AU, APQ8098, Kamorta, MDM9206, MDM9207C, MDM9607, MSM8905, MSM8909W, MSM8917, MSM8920, MSM8937, MSM8940, MSM8953, MSM8996, MSM8996AU, MSM8998, Nicobar, QCA6574AU, QCM2150, QCS405, QCS605, QM215, Rennell, SA6155P, Saipan, SDA660, SDA845, SDM429, SDM429W, SDM439, SDM450, SDM630, SDM632, SDM636, SDM660, SDM670, SDM710, SDM845, SDX20, SM6150, SM7150, SM8150, SM8250, SXR1130, SXR2130 **CVE ID : CVE-2020-3688**	https://www.qualcomm.com/company/product-security/bulletins/july-2020-bulletin	O-QUA-SDM6-190820/949
Out-of-bounds Write	30-Jul-20	7.5	Out of bound write while QoS DSCP mapping due to improper input validation for data received from association response	https://www.qualcomm.com/company/product-security/bull	O-QUA-SDM6-190820/950

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			frame 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, APQ8098, MDM9150, MDM9206, MDM9207C, MDM9607, MDM9650, MSM8905, MSM8909W, MSM8917, MSM8920, MSM8937, MSM8940, MSM8953, MSM8996AU, Nicobar, QCA6174A, QCA6574AU, QCA9377, QCA9379, QCM2150, QCN7605, QCS405, QCS605, QM215, SA6155P, Saipan, SC8180X, SDA845, SDM429, SDM429W, SDM439, SDM450, SDM630, SDM632, SDM636, SDM660, SDM845, SDX20, SDX55, SM8150, SM8250, SXR2130 **CVE ID : CVE-2020-3698**	etins/july-2020-bulletin	
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	30-Jul-20	7.5	Possible out of bound access while processing assoc response from host due to improper length check before copying into buffer in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer Electronics Connectivity,	https://www.qualcomm.com/company/product-security/bulletins/july-2020-bulletin	O-QUA-SDM6-190820/951

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, Nicobar, QCA6174A, QCA6574AU, QCA9377, QCA9379, QCM2150, QCN7605, QCS405, QCS605, QM215, SA6155P, Saipan, SC8180X, SDA845, SDM429, SDM429W, SDM439, SDM450, SDM630, SDM632, SDM636, SDM660, SDM845, SDX20, SDX55, SM6150, SM7150, SM8150, SM8250, SXR2130 **CVE ID : CVE-2020-3699**		
sdm660_firmware					
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	30-Jul-20	7.5	Possible buffer overflow while parsing mp4 clip with corrupted sample atoms due to improper validation of index in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial	https://www.qualcomm.com/company/product-security/bulletins/july-2020-bulletin	O-QUA-SDM6-190820/952

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables in APQ8009, APQ8017, APQ8053, APQ8096AU, APQ8098, Kamorta, MDM9206, MDM9207C, MDM9607, MSM8905, MSM8909W, MSM8917, MSM8920, MSM8937, MSM8940, MSM8953, MSM8996, MSM8996AU, MSM8998, Nicobar, QCA6574AU, QCM2150, QCS405, QCS605, QM215, Rennell, SA6155P, Saipan, SDA660, SDA845, SDM429, SDM429W, SDM439, SDM450, SDM630, SDM632, SDM636, SDM660, SDM670, SDM710, SDM845, SDX20, SM6150, SM7150, SM8150, SM8250, SXR1130, SXR2130 **CVE ID : CVE-2020-3688**		
Out-of-bounds Write	30-Jul-20	7.5	Out of bound write while QoS DSCP mapping due to improper input validation for data received from association response frame 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,	https://www.qualcomm.com/company/product-security/bulletins/july-2020-bulletin	O-QUA-SDM6-190820/953

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			APQ8053, APQ8096AU, APQ8098, MDM9150, MDM9206, MDM9207C, MDM9607, MDM9650, MSM8905, MSM8909W, MSM8917, MSM8920, MSM8937, MSM8940, MSM8953, MSM8996AU, Nicobar, QCA6174A, QCA6574AU, QCA9377, QCA9379, QCM2150, QCN7605, QCS405, QCS605, QM215, SA6155P, Saipan, SC8180X, SDA845, SDM429, SDM429W, SDM439, SDM450, SDM630, SDM632, SDM636, SDM660, SDM845, SDX20, SDX55, SM8150, SM8250, SXR2130 **CVE ID : CVE-2020-3698**		
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	30-Jul-20	7.5	Possible out of bound access while processing assoc response from host due to improper length check before copying into buffer 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,	https://www.qualcomm.com/company/product-security/bulletins/july-2020-bulletin	O-QUA-SDM6-190820/954

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			MSM8909W, MSM8917, MSM8920, MSM8937, MSM8940, MSM8953, MSM8996AU, Nicobar, QCA6174A, QCA6574AU, QCA9377, QCA9379, QCM2150, QCN7605, QCS405, QCS605, QM215, SA6155P, Saipan, SC8180X, SDA845, SDM429, SDM429W, SDM439, SDM450, SDM630, SDM632, SDM636, SDM660, SDM845, SDX20, SDX55, SM6150, SM7150, SM8150, SM8250, SXR2130 **CVE ID : CVE-2020-3699**		
mdm9150_firmware					
Out-of-bounds Write	30-Jul-20	7.5	Out of bound write while QoS DSCP mapping due to improper input validation for data received from association response frame 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, APQ8098, MDM9150, MDM9206, MDM9207C, MDM9607, MDM9650, MSM8905, MSM8909W,	https://www.qualcomm.com/company/product-security/bulletins/july-2020-bulletin	O-QUA-MDM9-190820/955

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			MSM8917, MSM8920, MSM8937, MSM8940, MSM8953, MSM8996AU, Nicobar, QCA6174A, QCA6574AU, QCA9377, QCA9379, QCM2150, QCN7605, QCS405, QCS605, QM215, SA6155P, Saipan, SC8180X, SDA845, SDM429, SDM429W, SDM439, SDM450, SDM630, SDM632, SDM636, SDM660, SDM845, SDX20, SDX55, SM8150, SM8250, SXR2130 **CVE ID : CVE-2020-3698**		
mdm9640_firmware					
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	30-Jul-20	7.5	Possible out of bound access while processing assoc response from host due to improper length check before copying into buffer 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,	https://www.qualcomm.com/company/product-security/bulletins/july-2020-bulletin	O-QUA-MDM9-190820/956

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			MSM8996AU, Nicobar, QCA6174A, QCA6574AU, QCA9377, QCA9379, QCM2150, QCN7605, QCS405, QCS605, QM215, SA6155P, Saipan, SC8180X, SDA845, SDM429, SDM429W, SDM439, SDM450, SDM630, SDM632, SDM636, SDM660, SDM845, SDX20, SDX55, SM6150, SM7150, SM8150, SM8250, SXR2130 **CVE ID : CVE-2020-3699**		
msm8909w_firmware					
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	30-Jul-20	7.5	Possible buffer overflow while parsing mp4 clip with corrupted sample atoms due to improper validation of index in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables in APQ8009, APQ8017, APQ8053, APQ8096AU, APQ8098, Kamorta, MDM9206, MDM9207C, MDM9607, MSM8905, MSM8909W, MSM8917, MSM8920, MSM8937, MSM8940, MSM8953, MSM8996, MSM8996AU, MSM8998, Nicobar,	https://www.qualcomm.com/company/product-security/bulletins/july-2020-bulletin	O-QUA-MSM8-190820/957

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			QCA6574AU, QCM2150, QCS405, QCS605, QM215, Rennell, SA6155P, Saipan, SDA660, SDA845, SDM429, SDM429W, SDM439, SDM450, SDM630, SDM632, SDM636, SDM660, SDM670, SDM710, SDM845, SDX20, SM6150, SM7150, SM8150, SM8250, SXR1130, SXR2130 **CVE ID : CVE-2020-3688**		
Out-of-bounds Write	30-Jul-20	7.5	Out of bound write while QoS DSCP mapping due to improper input validation for data received from association response frame 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, APQ8098, MDM9150, MDM9206, MDM9207C, MDM9607, MDM9650, MSM8905, MSM8909W, MSM8917, MSM8920, MSM8937, MSM8940, MSM8953, MSM8996AU, Nicobar, QCA6174A, QCA6574AU, QCA9377, QCA9379, QCM2150, QCN7605, QCS405, QCS605, QM215, SA6155P,	https://www.qualcomm.com/company/product-security/bulletins/july-2020-bulletin	O-QUA-MSM8-190820/958

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Saipan, SC8180X, SDA845, SDM429, SDM429W, SDM439, SDM450, SDM630, SDM632, SDM636, SDM660, SDM845, SDX20, SDX55, SM8150, SM8250, SXR2130 **CVE ID : CVE-2020-3698**		
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	30-Jul-20	7.5	Possible out of bound access while processing assoc response from host due to improper length check before copying into buffer 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, Nicobar, QCA6174A, QCA6574AU, QCA9377, QCA9379, QCM2150, QCN7605, QCS405, QCS605, QM215, SA6155P, Saipan, SC8180X, SDA845, SDM429, SDM429W, SDM439, SDM450, SDM630, SDM632,	https://www.qualcomm.com/company/product-security/bulletins/july-2020-bulletin	O-QUA-MSM8-190820/959

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			SDM636, SDM660, SDM845, SDX20, SDX55, SM6150, SM7150, SM8150, SM8250, SXR2130 **CVE ID : CVE-2020-3699**		
Out-of-bounds Read	30-Jul-20	5	Possible out of bounds read due to a missing bounds check and could lead to local information disclosure in the wifi driver with no additional execution privileges needed in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking in APQ8053, APQ8096AU, IPQ4019, IPQ8064, IPQ8074, MDM9607, MSM8909W, MSM8996AU, QCA6574AU, QCA9531, QCA9558, QCA9980, SC8180X, SDM439, SDX55, SM8150, SM8250, SXR2130 **CVE ID : CVE-2020-3700**	https://www.qualcomm.com/company/product-security/bulletins/july-2020-bulletin	O-QUA-MSM8-190820/960
qcs605_firmware					
Buffer Copy without Checking Size of Input ('Classic Buffer	30-Jul-20	7.5	Possible buffer overflow while parsing mp4 clip with corrupted sample atoms due to improper validation of index in Snapdragon Auto,	https://www.qualcomm.com/company/product-security/bulletins/july-	O-QUA-QCS6-190820/961

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Overflow')			Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables in APQ8009, APQ8017, APQ8053, APQ8096AU, APQ8098, Kamorta, MDM9206, MDM9207C, MDM9607, MSM8905, MSM8909W, MSM8917, MSM8920, MSM8937, MSM8940, MSM8953, MSM8996, MSM8996AU, MSM8998, Nicobar, QCA6574AU, QCM2150, QCS405, QCS605, QM215, Rennell, SA6155P, Saipan, SDA660, SDA845, SDM429, SDM429W, SDM439, SDM450, SDM630, SDM632, SDM636, SDM660, SDM670, SDM710, SDM845, SDX20, SM6150, SM7150, SM8150, SM8250, SXR1130, SXR2130 **CVE ID : CVE-2020-3688**	2020-bulletin	
Out-of-bounds Write	30-Jul-20	7.5	Out of bound write while QoS DSCP mapping due to improper input validation for data received from association response frame in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial	https://www.qualcomm.com/company/product-security/bulletins/july-2020-bulletin	O-QUA-QCS6-190820/962

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables in APQ8009, APQ8017, APQ8053, APQ8096AU, APQ8098, MDM9150, MDM9206, MDM9207C, MDM9607, MDM9650, MSM8905, MSM8909W, MSM8917, MSM8920, MSM8937, MSM8940, MSM8953, MSM8996AU, Nicobar, QCA6174A, QCA6574AU, QCA9377, QCA9379, QCM2150, QCN7605, QCS405, QCS605, QM215, SA6155P, Saipan, SC8180X, SDA845, SDM429, SDM429W, SDM439, SDM450, SDM630, SDM632, SDM636, SDM660, SDM845, SDX20, SDX55, SM8150, SM8250, SXR2130 **CVE ID : CVE-2020-3698**		
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	30-Jul-20	7.5	Possible out of bound access while processing assoc response from host due to improper length check before copying into buffer 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,	https://www.qualcomm.com/company/product-security/bulletins/july-2020-bulletin	O-QUA-QCS6-190820/963

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			APQ8053, APQ8096AU, MDM9206, MDM9207C, MDM9607, MDM9640, MDM9650, MSM8905, MSM8909W, MSM8917, MSM8920, MSM8937, MSM8940, MSM8953, MSM8996AU, Nicobar, QCA6174A, QCA6574AU, QCA9377, QCA9379, QCM2150, QCN7605, QCS405, QCS605, QM215, SA6155P, Saipan, SC8180X, SDA845, SDM429, SDM429W, SDM439, SDM450, SDM630, SDM632, SDM636, SDM660, SDM845, SDX20, SDX55, SM6150, SM7150, SM8150, SM8250, SXR2130 **CVE ID : CVE-2020-3699**		
sdx20_firmware					
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	30-Jul-20	7.5	Possible buffer overflow while parsing mp4 clip with corrupted sample atoms due to improper validation of index in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables in APQ8009, APQ8017, APQ8053, APQ8096AU, APQ8098, Kamorta,	https://www.qualcomm.com/company/product-security/bulletins/july-2020-bulletin	O-QUA-SDX2-190820/964

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			MDM9206, MDM9207C, MDM9607, MSM8905, MSM8909W, MSM8917, MSM8920, MSM8937, MSM8940, MSM8953, MSM8996, MSM8996AU, MSM8998, Nicobar, QCA6574AU, QCM2150, QCS405, QCS605, QM215, Rennell, SA6155P, Saipan, SDA660, SDA845, SDM429, SDM429W, SDM439, SDM450, SDM630, SDM632, SDM636, SDM660, SDM670, SDM710, SDM845, SDX20, SM6150, SM7150, SM8150, SM8250, SXR1130, SXR2130 **CVE ID : CVE-2020-3688**		
Out-of-bounds Write	30-Jul-20	7.5	Out of bound write while QoS DSCP mapping due to improper input validation for data received from association response frame 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, APQ8098, MDM9150, MDM9206, MDM9207C, MDM9607, MDM9650, MSM8905, MSM8909W, MSM8917, MSM8920,	https://www.qualcomm.com/company/product-security/bulletins/july-2020-bulletin	O-QUA-SDX2-190820/965

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			MSM8937, MSM8940, MSM8953, MSM8996AU, Nicobar, QCA6174A, QCA6574AU, QCA9377, QCA9379, QCM2150, QCN7605, QCS405, QCS605, QM215, SA6155P, Saipan, SC8180X, SDA845, SDM429, SDM429W, SDM439, SDM450, SDM630, SDM632, SDM636, SDM660, SDM845, SDX20, SDX55, SM8150, SM8250, SXR2130 **CVE ID : CVE-2020-3698**		
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	30-Jul-20	7.5	Possible out of bound access while processing assoc response from host due to improper length check before copying into buffer 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, Nicobar, QCA6174A, QCA6574AU, QCA9377, QCA9379,	https://www.qualcomm.com/company/product-security/bulletins/july-2020-bulletin	O-QUA-SDX2-190820/966

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			QCM2150, QCN7605, QCS405, QCS605, QM215, SA6155P, Saipan, SC8180X, SDA845, SDM429, SDM429W, SDM439, SDM450, SDM630, SDM632, SDM636, SDM660, SDM845, SDX20, SDX55, SM6150, SM7150, SM8150, SM8250, SXR2130 **CVE ID : CVE-2020-3699**		
sm7150_firmware					
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	30-Jul-20	7.5	Possible buffer overflow while parsing mp4 clip with corrupted sample atoms due to improper validation of index in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables in APQ8009, APQ8017, APQ8053, APQ8096AU, APQ8098, Kamorta, MDM9206, MDM9207C, MDM9607, MSM8905, MSM8909W, MSM8917, MSM8920, MSM8937, MSM8940, MSM8953, MSM8996, MSM8996AU, MSM8998, Nicobar, QCA6574AU, QCM2150, QCS405, QCS605, QM215, Rennell, SA6155P, Saipan,	https://www.qualcomm.com/company/product-security/bulletins/july-2020-bulletin	O-QUA-SM71-190820/967

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			SDA660, SDA845, SDM429, SDM429W, SDM439, SDM450, SDM630, SDM632, SDM636, SDM660, SDM670, SDM710, SDM845, SDX20, SM6150, SM7150, SM8150, SM8250, SXR1130, SXR2130 **CVE ID : CVE-2020-3688**		
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	30-Jul-20	7.5	Possible out of bound access while processing assoc response from host due to improper length check before copying into buffer 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, Nicobar, QCA6174A, QCA6574AU, QCA9377, QCA9379, QCM2150, QCN7605, QCS405, QCS605, QM215, SA6155P, Saipan, SC8180X, SDA845, SDM429, SDM429W, SDM439, SDM450,	https://www.qualcomm.com/company/product-security/bulletins/july-2020-bulletin	O-QUA-SM71-190820/968

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			SDM630, SDM632, SDM636, SDM660, SDM845, SDX20, SDX55, SM6150, SM7150, SM8150, SM8250, SXR2130 **CVE ID : CVE-2020-3699**		
sxr1130_firmware					
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	30-Jul-20	7.5	Possible buffer overflow while parsing mp4 clip with corrupted sample atoms due to improper validation of index in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables in APQ8009, APQ8017, APQ8053, APQ8096AU, APQ8098, Kamorta, MDM9206, MDM9207C, MDM9607, MSM8905, MSM8909W, MSM8917, MSM8920, MSM8937, MSM8940, MSM8953, MSM8996, MSM8996AU, MSM8998, Nicobar, QCA6574AU, QCM2150, QCS405, QCS605, QM215, Rennell, SA6155P, Saipan, SDA660, SDA845, SDM429, SDM429W, SDM439, SDM450, SDM630, SDM632, SDM636, SDM660, SDM670, SDM710, SDM845, SDX20,	https://www.qualcomm.com/company/product-security/bulletins/july-2020-bulletin	O-QUA-SXR1-190820/969

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			SM6150, SM7150, SM8150, SM8250, SXR1130, SXR2130 **CVE ID : CVE-2020-3688**		
rennell_firmware					
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	30-Jul-20	7.5	Possible buffer overflow while parsing mp4 clip with corrupted sample atoms due to improper validation of index in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables in APQ8009, APQ8017, APQ8053, APQ8096AU, APQ8098, Kamorta, MDM9206, MDM9207C, MDM9607, MSM8905, MSM8909W, MSM8917, MSM8920, MSM8937, MSM8940, MSM8953, MSM8996, MSM8996AU, MSM8998, Nicobar, QCA6574AU, QCM2150, QCS405, QCS605, QM215, Rennell, SA6155P, Saipan, SDA660, SDA845, SDM429, SDM429W, SDM439, SDM450, SDM630, SDM632, SDM636, SDM660, SDM670, SDM710, SDM845, SDX20, SM6150, SM7150, SM8150, SM8250, SXR1130, SXR2130	https://www.qualcomm.com/company/product-security/bulletins/july-2020-bulletin	O-QUA-RENN-190820/970

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2020-3688		
saipan_firmware					
Use After Free	30-Jul-20	7.5	Use-after-free issue could occur due to dangling pointer when generating a frame buffer in OpenGL ES in Snapdragon Compute, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music in APQ8009, Nicobar, QCM2150, QCS405, Saipan, SDM845, SM8150, SM8250, SXR2130 **CVE ID : CVE-2020-3671**	https://www.qualcomm.com/company/product-security/bulletins/july-2020-bulletin	O-QUA-SAIP-190820/971
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	30-Jul-20	7.5	Possible buffer overflow while parsing mp4 clip with corrupted sample atoms due to improper validation of index in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables in APQ8009, APQ8017, APQ8053, APQ8096AU, APQ8098, Kamorta, MDM9206, MDM9207C, MDM9607, MSM8905, MSM8909W, MSM8917, MSM8920, MSM8937, MSM8940, MSM8953, MSM8996, MSM8996AU, MSM8998, Nicobar, QCA6574AU, QCM2150,	https://www.qualcomm.com/company/product-security/bulletins/july-2020-bulletin	O-QUA-SAIP-190820/972

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			QCS405, QCS605, QM215, Rennell, SA6155P, Saipan, SDA660, SDA845, SDM429, SDM429W, SDM439, SDM450, SDM630, SDM632, SDM636, SDM660, SDM670, SDM710, SDM845, SDX20, SM6150, SM7150, SM8150, SM8250, SXR1130, SXR2130 **CVE ID : CVE-2020-3688**		
Out-of-bounds Write	30-Jul-20	7.5	Out of bound write while QoS DSCP mapping due to improper input validation for data received from association response frame 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, APQ8098, MDM9150, MDM9206, MDM9207C, MDM9607, MDM9650, MSM8905, MSM8909W, MSM8917, MSM8920, MSM8937, MSM8940, MSM8953, MSM8996AU, Nicobar, QCA6174A, QCA6574AU, QCA9377, QCA9379, QCM2150, QCN7605, QCS405, QCS605, QM215, SA6155P, Saipan, SC8180X, SDA845,	https://www.qualcomm.com/company/product-security/bulletins/july-2020-bulletin	O-QUA-SAIP-190820/973

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			SDM429, SDM429W, SDM439, SDM450, SDM630, SDM632, SDM636, SDM660, SDM845, SDX20, SDX55, SM8150, SM8250, SXR2130 **CVE ID : CVE-2020-3698**		
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	30-Jul-20	7.5	Possible out of bound access while processing assoc response from host due to improper length check before copying into buffer 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, Nicobar, QCA6174A, QCA6574AU, QCA9377, QCA9379, QCM2150, QCN7605, QCS405, QCS605, QM215, SA6155P, Saipan, SC8180X, SDA845, SDM429, SDM429W, SDM439, SDM450, SDM630, SDM632, SDM636, SDM660,	https://www.qualcomm.com/company/product-security/bulletins/july-2020-bulletin	O-QUA-SAIP-190820/974

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			SDM845, SDX20, SDX55, SM6150, SM7150, SM8150, SM8250, SXR2130 **CVE ID : CVE-2020-3699**		
Use After Free	30-Jul-20	4.6	Use after free issue while processing error notification from camx driver due to not properly releasing the sequence data in Snapdragon Mobile in Saipan, SM8250, SXR2130 **CVE ID : CVE-2020-3701**	https://www.qualcomm.com/company/product-security/bulletins/july-2020-bulletin	O-QUA-SAIP-190820/975
kamorta_firmware					
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	30-Jul-20	7.5	Possible buffer overflow while parsing mp4 clip with corrupted sample atoms due to improper validation of index in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables in APQ8009, APQ8017, APQ8053, APQ8096AU, APQ8098, Kamorta, MDM9206, MDM9207C, MDM9607, MSM8905, MSM8909W, MSM8917, MSM8920, MSM8937, MSM8940, MSM8953, MSM8996, MSM8996AU, MSM8998, Nicobar, QCA6574AU, QCM2150, QCS405, QCS605, QM215,	https://www.qualcomm.com/company/product-security/bulletins/july-2020-bulletin	O-QUA-KAMO-190820/976

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Rennell, SA6155P, Saipan, SDA660, SDA845, SDM429, SDM429W, SDM439, SDM450, SDM630, SDM632, SDM636, SDM660, SDM670, SDM710, SDM845, SDX20, SM6150, SM7150, SM8150, SM8250, SXR1130, SXR2130 **CVE ID : CVE-2020-3688**		
qca9558_firmware					
Out-of-bounds Read	30-Jul-20	5	Possible out of bounds read due to a missing bounds check and could lead to local information disclosure in the wifi driver with no additional execution privileges needed in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking in APQ8053, APQ8096AU, IPQ4019, IPQ8064, IPQ8074, MDM9607, MSM8909W, MSM8996AU, QCA6574AU, QCA9531, QCA9558, QCA9980, SC8180X, SDM439, SDX55, SM8150, SM8250, SXR2130 **CVE ID : CVE-2020-3700**	https://www.qualcomm.com/company/product-security/bulletins/july-2020-bulletin	O-QUA-QCA9-190820/977

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Redhat					
enterprise_linux_eus					
Out-of-bounds Write	31-Jul-20	3.6	There is an issue on grub2 before version 2.06 at function read_section_as_string(). It expects a font name to be at max UINT32_MAX - 1 length in bytes but it doesn't verify it before proceed with buffer allocation to read the value from the font value. An attacker may leverage that by crafting a malicious font file which has a name with UINT32_MAX, leading to read_section_as_string() to an arithmetic overflow, zero-sized allocation and further heap-based buffer overflow. **CVE ID : CVE-2020-14310**	https://bugzilla.redhat.com/show_bug.cgi?id=CVE-2020-14310	O-RED-ENTE-190820/978
Out-of-bounds Write	31-Jul-20	3.6	There is an issue with grub2 before version 2.06 while handling symlink on ext filesystems. A filesystem containing a symbolic link with an inode size of UINT32_MAX causes an arithmetic overflow leading to a zero-sized memory allocation with subsequent heap-based buffer overflow. **CVE ID : CVE-2020-14311**	https://bugzilla.redhat.com/show_bug.cgi?id=CVE-2020-14311	O-RED-ENTE-190820/979
enterprise_linux_server_aus					
Out-of-bounds	31-Jul-20	3.6	There is an issue on grub2 before version 2.06 at	https://bugzilla.redhat.co	O-RED-ENTE-190820/980

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Write			function read_section_as_string(). It expects a font name to be at max UINT32_MAX - 1 length in bytes but it doesn't verify it before proceed with buffer allocation to read the value from the font value. An attacker may leverage that by crafting a malicious font file which has a name with UINT32_MAX, leading to read_section_as_string() to an arithmetic overflow, zero-sized allocation and further heap-based buffer overflow. **CVE ID : CVE-2020-14310**	m/show_bug.cgi?id=CVE-2020-14310	
Out-of-bounds Write	31-Jul-20	3.6	There is an issue with grub2 before version 2.06 while handling symlink on ext filesystems. A filesystem containing a symbolic link with an inode size of UINT32_MAX causes an arithmetic overflow leading to a zero-sized memory allocation with subsequent heap-based buffer overflow. **CVE ID : CVE-2020-14311**	https://bugzilla.redhat.com/show_bug.cgi?id=CVE-2020-14311	O-RED-ENTE-190820/981
enterprise_linux_server_tus					
Out-of-bounds Write	31-Jul-20	3.6	There is an issue on grub2 before version 2.06 at function read_section_as_string(). It expects a font name to be at max UINT32_MAX - 1 length in bytes but it	https://bugzilla.redhat.com/show_bug.cgi?id=CVE-2020-14310	O-RED-ENTE-190820/982

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			doesn't verify it before proceed with buffer allocation to read the value from the font value. An attacker may leverage that by crafting a malicious font file which has a name with UINT32_MAX, leading to read_section_as_string() to an arithmetic overflow, zero-sized allocation and further heap-based buffer overflow. **CVE ID : CVE-2020-14310**		
Out-of-bounds Write	31-Jul-20	3.6	There is an issue with grub2 before version 2.06 while handling symlink on ext filesystems. A filesystem containing a symbolic link with an inode size of UINT32_MAX causes an arithmetic overflow leading to a zero-sized memory allocation with subsequent heap-based buffer overflow. **CVE ID : CVE-2020-14311**	https://bugzilla.redhat.com/show_bug.cgi?id=CVE-2020-14311	O-RED-ENTE-190820/983
enterprise_linux					
Out-of-bounds Write	31-Jul-20	3.6	There is an issue on grub2 before version 2.06 at function read_section_as_string(). It expects a font name to be at max UINT32_MAX - 1 length in bytes but it doesn't verify it before proceed with buffer allocation to read the value from the font value. An attacker may leverage that	https://bugzilla.redhat.com/show_bug.cgi?id=CVE-2020-14310	O-RED-ENTE-190820/984

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			by crafting a malicious font file which has a name with UINT32_MAX, leading to read_section_as_string() to an arithmetic overflow, zero-sized allocation and further heap-based buffer overflow. **CVE ID : CVE-2020-14310**		
Out-of-bounds Write	31-Jul-20	3.6	There is an issue with grub2 before version 2.06 while handling symlink on ext filesystems. A filesystem containing a symbolic link with an inode size of UINT32_MAX causes an arithmetic overflow leading to a zero-sized memory allocation with subsequent heap-based buffer overflow. **CVE ID : CVE-2020-14311**	https://bugzilla.redhat.com/show_bug.cgi?id=CVE-2020-14311	O-RED-ENTE-190820/985
Improper Verification of Cryptographic Signature	29-Jul-20	4.4	GRUB2 fails to validate kernel signature when booted directly without shim, allowing secure boot to be bypassed. This only affects systems where the kernel signing certificate has been imported directly into the secure boot database and the GRUB image is booted directly without the use of shim. This issue affects GRUB2 version 2.04 and prior versions. **CVE ID : CVE-2020-15705**	https://lists.gnu.org/archive/html/grub-devel/2020-07/msg00034.html, https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/ADV200011, https://security.netapp.com/advisory/ntap-	O-RED-ENTE-190820/986

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
				20200731-0008/	
Concurrent Execution using Shared Resource with Improper Synchronization ('Race Condition')	29-Jul-20	4.4	GRUB2 contains a race condition in grub_script_function_create() leading to a use-after-free vulnerability which can be triggered by redefining a function whilst the same function is already executing, leading to arbitrary code execution and secure boot restriction bypass. This issue affects GRUB2 version 2.04 and prior versions. **CVE ID : CVE-2020-15706**	https://lists.gnu.org/archive/html/grub-devel/2020-07/msg00034.html, https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/ADV200011, https://security.netapp.com/advisory/ntap-20200731-0008/	O-RED-ENTE-190820/987
Concurrent Execution using Shared Resource with Improper Synchronization ('Race Condition')	29-Jul-20	4.4	Integer overflows were discovered in the functions grub_cmd_initrd and grub_initrd_init in the efilinux component of GRUB2, as shipped in Debian, Red Hat, and Ubuntu (the functionality is not included in GRUB2 upstream), leading to a heap-based buffer overflow. These could be triggered by an extremely large number of arguments to the initrd command on 32-bit architectures, or a crafted filesystem with very large files on any architecture.	https://lists.gnu.org/archive/html/grub-devel/2020-07/msg00034.html, https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/ADV200011, https://security.netapp.com/advisory/ntap-20200731-	O-RED-ENTE-190820/988

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			An attacker could use this to execute arbitrary code and bypass UEFI Secure Boot restrictions. This issue affects GRUB2 version 2.04 and prior versions. **CVE ID : CVE-2020-15707**	0008/	
Ruckuswireless					
unleashed_firmware					
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	28-Jul-20	4.3	An XSS issue in emfd in Ruckus Wireless Unleashed through 200.7.10.102.92 allows a remote attacker to execute JavaScript code via an unauthenticated crafted HTTP request. This affects C110, E510, H320, H510, M510, R320, R310, R500, R510 R600, R610, R710, R720, R750, T300, T301n, T301s, T310c, T310d, T310n, T310s, T610, T710, and T710s devices. **CVE ID : CVE-2020-13913**	https://support.ruckuswireless.com/security_bulletins/304	O-RUC-UNLE-190820/989
Improper Input Validation	28-Jul-20	5	webs in Ruckus Wireless Unleashed through 200.7.10.102.92 allows a remote attacker to cause a denial of service (Segmentation fault) to the webserver via an unauthenticated crafted HTTP request. This affects C110, E510, H320, H510, M510, R320, R310, R500, R510 R600, R610, R710, R720, R750, T300, T301n,	https://support.ruckuswireless.com/security_bulletins/304	O-RUC-UNLE-190820/990

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			T301s, T310c, T310d, T310n, T310s, T610, T710, and T710s devices. **CVE ID : CVE-2020-13914**		
Insufficiently Protected Credentials	28-Jul-20	6.4	Insecure permissions in emfd/libemf in Ruckus Wireless Unleashed through 200.7.10.102.92 allow a remote attacker to overwrite admin credentials via an unauthenticated crafted HTTP request. This affects C110, E510, H320, H510, M510, R320, R310, R500, R510 R600, R610, R710, R720, R750, T300, T301n, T301s, T310c, T310d, T310n, T310s, T610, T710, and T710s devices. **CVE ID : CVE-2020-13915**	https://support.ruckuswireless.com/security_bulletins/304	O-RUC-UNLE-190820/991
Out-of-bounds Write	28-Jul-20	7.5	A stack buffer overflow in webs in Ruckus Wireless Unleashed through 200.7.10.102.92 allows a remote attacker to execute code via an unauthenticated crafted HTTP request. This affects C110, E510, H320, H510, M510, R320, R310, R500, R510 R600, R610, R710, R720, R750, T300, T301n, T301s, T310c, T310d, T310n, T310s, T610, T710, and T710s devices. **CVE ID : CVE-2020-13916**	https://support.ruckuswireless.com/security_bulletins/304	O-RUC-UNLE-190820/992
Improper Neutralizatio	28-Jul-20	7.5	rkscli in Ruckus Wireless Unleashed through	https://support.ruckuswi	O-RUC-UNLE-190820/993

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
n of Special Elements used in an OS Command ('OS Command Injection')			200.7.10.92 allows a remote attacker to achieve command injection and jailbreak the CLI via a crafted CLI command. This affects C110, E510, H320, H510, M510, R320, R310, R500, R510 R600, R610, R710, R720, R750, T300, T301n, T301s, T310c, T310d, T310n, T310s, T610, T710, and T710s devices. **CVE ID : CVE-2020-13917**	reless.com/security_bulletins/304	
Information Exposure	28-Jul-20	5	Incorrect access control in webs in Ruckus Wireless Unleashed through 200.7.10.102.92 allows a remote attacker to leak system information (that can be used for a jailbreak) via an unauthenticated crafted HTTP request. This affects C110, E510, H320, H510, M510, R320, R310, R500, R510 R600, R610, R710, R720, R750, T300, T301n, T301s, T310c, T310d, T310n, T310s, T610, T710, and T710s devices. **CVE ID : CVE-2020-13918**	https://support.ruckuswireless.com/security_bulletins/304	O-RUC-UNLE-190820/994
Improper Neutralization of Special Elements used in an OS Command ('OS Command	28-Jul-20	7.5	emfd/libemf in Ruckus Wireless Unleashed through 200.7.10.102.92 allows a remote attacker to achieve command injection via a crafted HTTP request. This affects C110, E510, H320, H510,	https://support.ruckuswireless.com/security_bulletins/304	O-RUC-UNLE-190820/995

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Injection')			M510, R320, R310, R500, R510 R600, R610, R710, R720, R750, T300, T301n, T301s, T310c, T310d, T310n, T310s, T610, T710, and T710s devices. **CVE ID : CVE-2020-13919**		
Schneider-electric					
tricon_tcm_4351_firmware					
Information Exposure	23-Jul-20	5	**VERSION NOT SUPPORTED WHEN ASSIGNED** A legacy debug port account in TCMs installed in Tricon system versions 10.2.0 through 10.5.3 is visible on the network and could allow inappropriate access. This vulnerability was remediated in TCM version 10.5.4. **CVE ID : CVE-2020-7491**	N/A	O-SCH-TRIC-190820/996
tricon_tcm_4352_firmware					
Information Exposure	23-Jul-20	5	**VERSION NOT SUPPORTED WHEN ASSIGNED** A legacy debug port account in TCMs installed in Tricon system versions 10.2.0 through 10.5.3 is visible on the network and could allow inappropriate access. This vulnerability was remediated in TCM version 10.5.4. **CVE ID : CVE-2020-7491**	N/A	O-SCH-TRIC-190820/997
tricon_tcm_4351a_firmware					
Information	23-Jul-20	5	**VERSION NOT	N/A	O-SCH-TRIC-

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Exposure			SUPPORTED WHEN ASSIGNED** A legacy debug port account in TCMs installed in Tricon system versions 10.2.0 through 10.5.3 is visible on the network and could allow inappropriate access. This vulnerability was remediated in TCM version 10.5.4. **CVE ID : CVE-2020-7491**		190820/998
tricon_tcm_4351b_firmware					
Information Exposure	23-Jul-20	5	**VERSION NOT SUPPORTED WHEN ASSIGNED** A legacy debug port account in TCMs installed in Tricon system versions 10.2.0 through 10.5.3 is visible on the network and could allow inappropriate access. This vulnerability was remediated in TCM version 10.5.4. **CVE ID : CVE-2020-7491**	N/A	O-SCH-TRIC-190820/999
tricon_tcm_4352a_firmware					
Information Exposure	23-Jul-20	5	**VERSION NOT SUPPORTED WHEN ASSIGNED** A legacy debug port account in TCMs installed in Tricon system versions 10.2.0 through 10.5.3 is visible on the network and could allow inappropriate access. This vulnerability was remediated in TCM version 10.5.4.	N/A	O-SCH-TRIC-190820/1000

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2020-7491		
tricon_tcm_4352b_firmware					
Information Exposure	23-Jul-20	5	**VERSION NOT SUPPORTED WHEN ASSIGNED** A legacy debug port account in TCMs installed in Tricon system versions 10.2.0 through 10.5.3 is visible on the network and could allow inappropriate access. This vulnerability was remediated in TCM version 10.5.4. **CVE ID : CVE-2020-7491**	N/A	O-SCH-TRIC-190820/1001
Sonicwall					
sonicos					
Improper Input Validation	17-Jul-20	5	SonicOS SSLVPN LDAP login request allows remote attackers to cause external service interaction (DNS) due to improper validation of the request. This vulnerability impact SonicOS version 6.5.4.4-44n and earlier. **CVE ID : CVE-2020-5130**	https://psirt.global.sonicwall.com/vuln-detail/SNWLID-2020-0003	O-SON-SONI-190820/1002
Suse					
suse_linux_enterprise_server					
Improper Verification of Cryptographic Signature	29-Jul-20	4.4	GRUB2 fails to validate kernel signature when booted directly without shim, allowing secure boot to be bypassed. This only affects systems where the kernel signing certificate has been imported directly into the secure boot	https://lists.gnu.org/archive/html/grub-devel/2020-07/msg00034.html, https://portal.msrc.micr	O-SUS-SUSE-190820/1003

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			database and the GRUB image is booted directly without the use of shim. This issue affects GRUB2 version 2.04 and prior versions. **CVE ID : CVE-2020-15705**	osoft.com/en-US/security-guidance/advisory/ADV200011, https://security.netapp.com/advisory/ntap-20200731-0008/	
Concurrent Execution using Shared Resource with Improper Synchronization ('Race Condition')	29-Jul-20	4.4	GRUB2 contains a race condition in grub_script_function_create() leading to a use-after-free vulnerability which can be triggered by redefining a function whilst the same function is already executing, leading to arbitrary code execution and secure boot restriction bypass. This issue affects GRUB2 version 2.04 and prior versions. **CVE ID : CVE-2020-15706**	https://lists.gnu.org/archive/html/grub-devel/2020-07/msg00034.html, https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/ADV200011, https://security.netapp.com/advisory/ntap-20200731-0008/	O-SUS-SUSE-190820/1004
Concurrent Execution using Shared Resource with Improper Synchronization ('Race Condition')	29-Jul-20	4.4	Integer overflows were discovered in the functions grub_cmd_initrd and grub_initrd_init in the efilinux component of GRUB2, as shipped in Debian, Red Hat, and Ubuntu (the functionality is not included in GRUB2 upstream), leading to a	https://lists.gnu.org/archive/html/grub-devel/2020-07/msg00034.html, https://portal.msrc.microsoft.com/en	O-SUS-SUSE-190820/1005

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			heap-based buffer overflow. These could be triggered by an extremely large number of arguments to the initrd command on 32-bit architectures, or a crafted filesystem with very large files on any architecture. An attacker could use this to execute arbitrary code and bypass UEFI Secure Boot restrictions. This issue affects GRUB2 version 2.04 and prior versions. **CVE ID : CVE-2020-15707**	-US/security-guidance/advisory/ADV200011, https://security.netapp.com/advisory/ntap-20200731-0008/	
teltonika-networks					
gateway_trb245_firmware					
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	17-Jul-20	3.5	Insufficient output sanitization in Teltonika firmware TRB2_R_00.02.02 allows a remote, authenticated attacker to conduct persistent cross-site scripting (XSS) attacks by injecting malicious client-side code into the 'URL/ Host / Connection' form in the 'DATA TO SERVER' configuration section. **CVE ID : CVE-2020-5769**	https://www.tenable.com/security/research/tra-2020-43-0	O-TEL-GATE-190820/1006
Tenda					
ac15_firmware					
Improper Neutralization of Special Elements	23-Jul-20	10	goform/AdvSetLanip endpoint on Tenda AC15 AC1900 15.03.05.19 devices allows remote	N/A	O-TEN-AC15-190820/1007

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
used in an OS Command ('OS Command Injection')			attackers to execute arbitrary system commands via shell metacharacters in the lanIp POST parameter. **CVE ID : CVE-2020-15916**		
Tesla					
model_3_firmware					
N/A	23-Jul-20	3.3	** DISPUTED ** Tesla Model 3 vehicles allow attackers to open a door by leveraging access to a legitimate key card, and then using NFC Relay. NOTE: the vendor has developed Pin2Drive to mitigate this issue. **CVE ID : CVE-2020-15912**	N/A	O-TES-MODE-190820/1008
Veeam					
one_firmware					
Improper Restriction of XML External Entity Reference ('XXE')	28-Jul-20	7.8	This vulnerability allows remote attackers to disclose sensitive information on affected installations of Veeam ONE 10.0.0.750_20200415. Authentication is not required to exploit this vulnerability. The specific flaw exists within the SSRSReport class. Due to the improper restriction of XML External Entity (XXE) references, a specially crafted document specifying a URI causes the XML parser to access the URI and embed the contents back into the XML	N/A	O-VEE-ONE_-190820/1009

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			document for further processing. An attacker can leverage this vulnerability to disclose file contents in the context of SYSTEM. Was ZDI-CAN-10709. **CVE ID : CVE-2020-15418**		
Improper Restriction of XML External Entity Reference ('XXE')	28-Jul-20	7.8	This vulnerability allows remote attackers to disclose sensitive information on affected installations of Veeam ONE 10.0.0.750_20200415. Authentication is not required to exploit this vulnerability. The specific flaw exists within the Reporter_ImportLicense class. Due to the improper restriction of XML External Entity (XXE) references, a specially crafted document specifying a URI causes the XML parser to access the URI and embed the contents back into the XML document for further processing. An attacker can leverage this vulnerability to disclose file contents in the context of SYSTEM. Was ZDI-CAN-10710. **CVE ID : CVE-2020-15419**	N/A	O-VEE-ONE_-190820/1010
Windriver					
vxworks					
Information Exposure	23-Jul-20	5	httpRpmFs in WebCLI in Wind River VxWorks 5.5	N/A	O-WIN-VXWO-

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			through 7 SR0640 has no check for an escape from the web root. **CVE ID : CVE-2020-11440**		190820/1011
XEN					
xen					
Incorrect Default Permissions	20-Jul-20	4.6	An issue was discovered in the Linux kernel 5.5 through 5.7.9, as used in Xen through 4.13.x for x86 PV guests. An attacker may be granted the I/O port permissions of an unrelated task. This occurs because tss_invalidate_io_bitmap mishandling causes a loss of synchronization between the I/O bitmaps of TSS and Xen, aka CID-cadfad870154. **CVE ID : CVE-2020-15852**	https://security.netapp.com/advisory/ntap-20200810-0001/	O-XEN-XEN-190820/1012
ZTE					
r8500g4_firmware					
Improper Authentication	20-Jul-20	7.5	The server management software module of ZTE has an authentication issue vulnerability, which allows users to skip the authentication of the server and execute some commands for high-level users. This affects: <R5300G4V03.08.0100/V03.07.0300/V03.07.0200/V03.07.0108/V03.07.0100/V03.05.0047/V03.05.0046/V03.05.0045/V03.05.0044/V03.05.0043/V03.05.0	N/A	O-ZTE-R850-190820/1013

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			040/V03.04.0020;R8500G4V03.07.0103/V03.07.0101/V03.06.0100/V03.05.0400/V03.05.0020;R5500G4V03.08.0100/V03.07.0200/V03.07.0100/V03.06.0100> **CVE ID : CVE-2020-6871**		
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	20-Jul-20	4.3	The server management software module of ZTE has a storage XSS vulnerability. The attacker inserts some attack codes through the foreground login page, which will cause the user to execute the predefined malicious script in the browser. This affects <R5300G4V03.08.0100/V03.07.0300/V03.07.0200/V03.07.0108/V03.07.0100/V03.05.0047/V03.05.0046/V03.05.0045/V03.05.0044/V03.05.0043/V03.05.0040/V03.04.0020;R8500G4V03.07.0103/V03.07.0101/V03.06.0100/V03.05.0400/V03.05.0020;R5500G4V03.08.0100/V03.07.0200/V03.07.0100/V03.06.0100>. **CVE ID : CVE-2020-6872**	N/A	O-ZTE-R850-190820/1014
r5500g4_firmware					
Improper Authentication	20-Jul-20	7.5	The server management software module of ZTE has an authentication issue vulnerability, which allows users to skip the authentication of the	N/A	O-ZTE-R550-190820/1015

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			server and execute some commands for high-level users. This affects: <R5300G4V03.08.0100/V03.07.0300/V03.07.0200/V03.07.0108/V03.07.0100/V03.05.0047/V03.05.0046/V03.05.0045/V03.05.0044/V03.05.0043/V03.05.0040/V03.04.0020;R8500G4V03.07.0103/V03.07.0101/V03.06.0100/V03.05.0400/V03.05.0020;R5500G4V03.08.0100/V03.07.0200/V03.07.0100/V03.06.0100> **CVE ID : CVE-2020-6871**		
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	20-Jul-20	4.3	The server management software module of ZTE has a storage XSS vulnerability. The attacker inserts some attack codes through the foreground login page, which will cause the user to execute the predefined malicious script in the browser. This affects <R5300G4V03.08.0100/V03.07.0300/V03.07.0200/V03.07.0108/V03.07.0100/V03.05.0047/V03.05.0046/V03.05.0045/V03.05.0044/V03.05.0043/V03.05.0040/V03.04.0020;R8500G4V03.07.0103/V03.07.0101/V03.06.0100/V03.05.0400/V03.05.0020;R5500G4V03.08.0100/V03.07.0200/V03.07.0100/V03.06.010	N/A	O-ZTE-R550-190820/1016

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			0>. **CVE ID : CVE-2020-6872**		
r5300g4_firmware					
Improper Authentication	20-Jul-20	7.5	The server management software module of ZTE has an authentication issue vulnerability, which allows users to skip the authentication of the server and execute some commands for high-level users. This affects: <R5300G4V03.08.0100/V03.07.0300/V03.07.0200/V03.07.0108/V03.07.0100/V03.05.0047/V03.05.0046/V03.05.0045/V03.05.0044/V03.05.0043/V03.05.0040/V03.04.0020;R8500G4V03.07.0103/V03.07.0101/V03.06.0100/V03.05.0400/V03.05.0020;R5500G4V03.08.0100/V03.07.0200/V03.07.0100/V03.06.0100> **CVE ID : CVE-2020-6871**	N/A	O-ZTE-R530-190820/1017
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	20-Jul-20	4.3	The server management software module of ZTE has a storage XSS vulnerability. The attacker inserts some attack codes through the foreground login page, which will cause the user to execute the predefined malicious script in the browser. This affects <R5300G4V03.08.0100/V03.07.0300/V03.07.0200/V03.07.0108/V03.07.0100	N/A	O-ZTE-R530-190820/1018

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			/V03.05.0047/V03.05.0046/V03.05.0045/V03.05.0044/V03.05.0043/V03.05.0040/V03.04.0020;R8500G4V03.07.0103/V03.07.0101/V03.06.0100/V03.05.0400/V03.05.0020;R5500G4V03.08.0100/V03.07.0200/V03.07.0100/V03.06.0100>. **CVE ID : CVE-2020-6872**		
Hardware					
abus					
secvest_hybrid_fumo50110					
Improper Authentication	30-Jul-20	6.4	The ABUS Secvest FUMO50110 hybrid module does not have any security mechanism that ensures confidentiality or integrity of RF packets that are exchanged with an alarm panel. This makes it easier to conduct wAppLoxx authentication-bypass attacks. **CVE ID : CVE-2020-14158**	N/A	H-ABU-SECV-190820/1019
automationdirect					
ea9-pgmsw					
Improper Authentication	23-Jul-20	5	This vulnerability allows remote attackers to bypass authentication on affected installations of C-MORE HMI EA9 Firmware version 6.52 touch screen panels. Authentication is not required to exploit this vulnerability. The specific flaw exists within the	N/A	H-AUT-EA9--190820/1020

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			authentication mechanism. The issue is due to insufficient authentication on post-authentication requests. An attacker can leverage this vulnerability to escalate privileges to resources normally protected from unauthenticated users. Was ZDI-CAN-10182. **CVE ID : CVE-2020-10918**		
Weak Cryptography for Passwords	23-Jul-20	4.3	This vulnerability allows remote attackers to disclose sensitive information on affected installations of C-MORE HMI EA9 Firmware version 6.52 touch screen panels. Authentication is not required to exploit this vulnerability. The specific flaw exists within the handling of passwords. When transmitting passwords, the process encrypts them in a recoverable format using a hard-coded key. An attacker can leverage this vulnerability to disclose credentials, leading to further compromise. Was ZDI-CAN-10185. **CVE ID : CVE-2020-10919**	N/A	H-AUT-EA9--190820/1021
Missing Authentication for Critical Function	23-Jul-20	7.5	This vulnerability allows remote attackers to execute arbitrary code on affected installations of C-MORE HMI EA9 Firmware	N/A	H-AUT-EA9--190820/1022

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			version 6.52 touch screen panels. Authentication is not required to exploit this vulnerability. The specific flaw exists within the control service, which listens on TCP port 9999 by default. The issue results from the lack of authentication prior to allowing alterations to the system configuration. An attacker can leverage this vulnerability to execute code in the context of the device. Was ZDI-CAN-10493. **CVE ID : CVE-2020-10920**		
Missing Authenticati on for Critical Function	23-Jul-20	7.5	This vulnerability allows remote attackers to issue commands on affected installations of C-MORE HMI EA9 Firmware version 6.52 touch screen panels. Authentication is not required to exploit this vulnerability. The specific flaw exists within the EA-HTTP.exe process. The issue results from the lack of authentication prior to allowing alterations to the system configuration. An attacker can leverage this vulnerability to issue commands to the physical equipment controlled by the device. Was ZDI-CAN-10482. **CVE ID : CVE-2020-10921**	N/A	H-AUT-EA9--190820/1023

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Improper Input Validation	23-Jul-20	5	This vulnerability allows remote attackers to create a denial-of-service condition on affected installations of C-MORE HMI EA9 Firmware version 6.52 touch screen panels. Authentication is not required to exploit this vulnerability. The specific flaw exists within the EA-HTTP.exe process. The issue results from the lack of proper input validation prior to further processing user requests. An attacker can leverage this vulnerability to create a denial-of-service condition on the system. Was ZDI-CAN-10527. **CVE ID : CVE-2020-10922**	N/A	H-AUT-EA9--190820/1024
ea9-rhmi					
Improper Authenticati on	23-Jul-20	5	This vulnerability allows remote attackers to bypass authentication on affected installations of C-MORE HMI EA9 Firmware version 6.52 touch screen panels. Authentication is not required to exploit this vulnerability. The specific flaw exists within the authentication mechanism. The issue is due to insufficient authentication on post-authentication requests. An attacker can leverage this vulnerability to escalate privileges to	N/A	H-AUT-EA9--190820/1025

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			resources normally protected from unauthenticated users. Was ZDI-CAN-10182. **CVE ID : CVE-2020-10918**		
Weak Cryptography for Passwords	23-Jul-20	4.3	This vulnerability allows remote attackers to disclose sensitive information on affected installations of C-MORE HMI EA9 Firmware version 6.52 touch screen panels. Authentication is not required to exploit this vulnerability. The specific flaw exists within the handling of passwords. When transmitting passwords, the process encrypts them in a recoverable format using a hard-coded key. An attacker can leverage this vulnerability to disclose credentials, leading to further compromise. Was ZDI-CAN-10185. **CVE ID : CVE-2020-10919**	N/A	H-AUT-EA9--190820/1026
Missing Authentication for Critical Function	23-Jul-20	7.5	This vulnerability allows remote attackers to execute arbitrary code on affected installations of C-MORE HMI EA9 Firmware version 6.52 touch screen panels. Authentication is not required to exploit this vulnerability. The specific flaw exists within the control service, which listens on TCP port 9999	N/A	H-AUT-EA9--190820/1027

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			by default. The issue results from the lack of authentication prior to allowing alterations to the system configuration. An attacker can leverage this vulnerability to execute code in the context of the device. Was ZDI-CAN-10493. **CVE ID : CVE-2020-10920**		
Missing Authentication for Critical Function	23-Jul-20	7.5	This vulnerability allows remote attackers to issue commands on affected installations of C-MORE HMI EA9 Firmware version 6.52 touch screen panels. Authentication is not required to exploit this vulnerability. The specific flaw exists within the EA-HTTP.exe process. The issue results from the lack of authentication prior to allowing alterations to the system configuration. An attacker can leverage this vulnerability to issue commands to the physical equipment controlled by the device. Was ZDI-CAN-10482. **CVE ID : CVE-2020-10921**	N/A	H-AUT-EA9--190820/1028
Improper Input Validation	23-Jul-20	5	This vulnerability allows remote attackers to create a denial-of-service condition on affected installations of C-MORE HMI EA9 Firmware version 6.52 touch screen	N/A	H-AUT-EA9--190820/1029

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			panels. Authentication is not required to exploit this vulnerability. The specific flaw exists within the EA-HTTP.exe process. The issue results from the lack of proper input validation prior to further processing user requests. An attacker can leverage this vulnerability to create a denial-of-service condition on the system. Was ZDI-CAN-10527. **CVE ID : CVE-2020-10922**		
ea9-t10cl					
Improper Authentication	23-Jul-20	5	This vulnerability allows remote attackers to bypass authentication on affected installations of C-MORE HMI EA9 Firmware version 6.52 touch screen panels. Authentication is not required to exploit this vulnerability. The specific flaw exists within the authentication mechanism. The issue is due to insufficient authentication on post-authentication requests. An attacker can leverage this vulnerability to escalate privileges to resources normally protected from unauthenticated users. Was ZDI-CAN-10182. **CVE ID : CVE-2020-10918**	N/A	H-AUT-EA9--190820/1030
Weak Cryptograph	23-Jul-20	4.3	This vulnerability allows remote attackers to	N/A	H-AUT-EA9--

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
y for Passwords			disclose sensitive information on affected installations of C-MORE HMI EA9 Firmware version 6.52 touch screen panels. Authentication is not required to exploit this vulnerability. The specific flaw exists within the handling of passwords. When transmitting passwords, the process encrypts them in a recoverable format using a hard-coded key. An attacker can leverage this vulnerability to disclose credentials, leading to further compromise. Was ZDI-CAN-10185. **CVE ID : CVE-2020-10919**		190820/1031
Missing Authenticati on for Critical Function	23-Jul-20	7.5	This vulnerability allows remote attackers to execute arbitrary code on affected installations of C-MORE HMI EA9 Firmware version 6.52 touch screen panels. Authentication is not required to exploit this vulnerability. The specific flaw exists within the control service, which listens on TCP port 9999 by default. The issue results from the lack of authentication prior to allowing alterations to the system configuration. An attacker can leverage this vulnerability to execute code in the context of the	N/A	H-AUT-EA9--190820/1032

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			device. Was ZDI-CAN-10493. **CVE ID : CVE-2020-10920**		
Missing Authentication for Critical Function	23-Jul-20	7.5	This vulnerability allows remote attackers to issue commands on affected installations of C-MORE HMI EA9 Firmware version 6.52 touch screen panels. Authentication is not required to exploit this vulnerability. The specific flaw exists within the EA-HTTP.exe process. The issue results from the lack of authentication prior to allowing alterations to the system configuration. An attacker can leverage this vulnerability to issue commands to the physical equipment controlled by the device. Was ZDI-CAN-10482. **CVE ID : CVE-2020-10921**	N/A	H-AUT-EA9--190820/1033
Improper Input Validation	23-Jul-20	5	This vulnerability allows remote attackers to create a denial-of-service condition on affected installations of C-MORE HMI EA9 Firmware version 6.52 touch screen panels. Authentication is not required to exploit this vulnerability. The specific flaw exists within the EA-HTTP.exe process. The issue results from the lack of proper input validation prior to further processing	N/A	H-AUT-EA9--190820/1034

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			user requests. An attacker can leverage this vulnerability to create a denial-of-service condition on the system. Was ZDI-CAN-10527. **CVE ID : CVE-2020-10922**		
ea9-t10wcl					
Improper Authentication	23-Jul-20	5	This vulnerability allows remote attackers to bypass authentication on affected installations of C-MORE HMI EA9 Firmware version 6.52 touch screen panels. Authentication is not required to exploit this vulnerability. The specific flaw exists within the authentication mechanism. The issue is due to insufficient authentication on post-authentication requests. An attacker can leverage this vulnerability to escalate privileges to resources normally protected from unauthenticated users. Was ZDI-CAN-10182. **CVE ID : CVE-2020-10918**	N/A	H-AUT-EA9--190820/1035
Weak Cryptography for Passwords	23-Jul-20	4.3	This vulnerability allows remote attackers to disclose sensitive information on affected installations of C-MORE HMI EA9 Firmware version 6.52 touch screen panels. Authentication is not required to exploit this vulnerability. The specific	N/A	H-AUT-EA9--190820/1036

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			flaw exists within the handling of passwords. When transmitting passwords, the process encrypts them in a recoverable format using a hard-coded key. An attacker can leverage this vulnerability to disclose credentials, leading to further compromise. Was ZDI-CAN-10185. **CVE ID : CVE-2020-10919**		
Missing Authenticati on for Critical Function	23-Jul-20	7.5	This vulnerability allows remote attackers to execute arbitrary code on affected installations of C-MORE HMI EA9 Firmware version 6.52 touch screen panels. Authentication is not required to exploit this vulnerability. The specific flaw exists within the control service, which listens on TCP port 9999 by default. The issue results from the lack of authentication prior to allowing alterations to the system configuration. An attacker can leverage this vulnerability to execute code in the context of the device. Was ZDI-CAN-10493. **CVE ID : CVE-2020-10920**	N/A	H-AUT-EA9--190820/1037
Missing Authenticati on for Critical	23-Jul-20	7.5	This vulnerability allows remote attackers to issue commands on affected installations of C-MORE	N/A	H-AUT-EA9--190820/1038

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Function			HMI EA9 Firmware version 6.52 touch screen panels. Authentication is not required to exploit this vulnerability. The specific flaw exists within the EA-HTTP.exe process. The issue results from the lack of authentication prior to allowing alterations to the system configuration. An attacker can leverage this vulnerability to issue commands to the physical equipment controlled by the device. Was ZDI-CAN-10482. **CVE ID : CVE-2020-10921**		
Improper Input Validation	23-Jul-20	5	This vulnerability allows remote attackers to create a denial-of-service condition on affected installations of C-MORE HMI EA9 Firmware version 6.52 touch screen panels. Authentication is not required to exploit this vulnerability. The specific flaw exists within the EA-HTTP.exe process. The issue results from the lack of proper input validation prior to further processing user requests. An attacker can leverage this vulnerability to create a denial-of-service condition on the system. Was ZDI-CAN-10527. **CVE ID : CVE-2020-10922**	N/A	H-AUT-EA9--190820/1039

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
ea9-t12cl					
Improper Authentication	23-Jul-20	5	This vulnerability allows remote attackers to bypass authentication on affected installations of C-MORE HMI EA9 Firmware version 6.52 touch screen panels. Authentication is not required to exploit this vulnerability. The specific flaw exists within the authentication mechanism. The issue is due to insufficient authentication on post-authentication requests. An attacker can leverage this vulnerability to escalate privileges to resources normally protected from unauthenticated users. Was ZDI-CAN-10182. **CVE ID : CVE-2020-10918**	N/A	H-AUT-EA9--190820/1040
Weak Cryptography for Passwords	23-Jul-20	4.3	This vulnerability allows remote attackers to disclose sensitive information on affected installations of C-MORE HMI EA9 Firmware version 6.52 touch screen panels. Authentication is not required to exploit this vulnerability. The specific flaw exists within the handling of passwords. When transmitting passwords, the process encrypts them in a recoverable format using a hard-coded key. An	N/A	H-AUT-EA9--190820/1041

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			attacker can leverage this vulnerability to disclose credentials, leading to further compromise. Was ZDI-CAN-10185. **CVE ID : CVE-2020-10919**		
Missing Authentication for Critical Function	23-Jul-20	7.5	This vulnerability allows remote attackers to execute arbitrary code on affected installations of C-MORE HMI EA9 Firmware version 6.52 touch screen panels. Authentication is not required to exploit this vulnerability. The specific flaw exists within the control service, which listens on TCP port 9999 by default. The issue results from the lack of authentication prior to allowing alterations to the system configuration. An attacker can leverage this vulnerability to execute code in the context of the device. Was ZDI-CAN-10493. **CVE ID : CVE-2020-10920**	N/A	H-AUT-EA9--190820/1042
Missing Authentication for Critical Function	23-Jul-20	7.5	This vulnerability allows remote attackers to issue commands on affected installations of C-MORE HMI EA9 Firmware version 6.52 touch screen panels. Authentication is not required to exploit this vulnerability. The specific flaw exists within the EA-HTTP.exe process. The	N/A	H-AUT-EA9--190820/1043

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			issue results from the lack of authentication prior to allowing alterations to the system configuration. An attacker can leverage this vulnerability to issue commands to the physical equipment controlled by the device. Was ZDI-CAN-10482. **CVE ID : CVE-2020-10921**		
Improper Input Validation	23-Jul-20	5	This vulnerability allows remote attackers to create a denial-of-service condition on affected installations of C-MORE HMI EA9 Firmware version 6.52 touch screen panels. Authentication is not required to exploit this vulnerability. The specific flaw exists within the EA-HTTP.exe process. The issue results from the lack of proper input validation prior to further processing user requests. An attacker can leverage this vulnerability to create a denial-of-service condition on the system. Was ZDI-CAN-10527. **CVE ID : CVE-2020-10922**	N/A	H-AUT-EA9--190820/1044
ea9-t15cl					
Improper Authenticati on	23-Jul-20	5	This vulnerability allows remote attackers to bypass authentication on affected installations of C-MORE HMI EA9 Firmware version 6.52 touch screen	N/A	H-AUT-EA9--190820/1045

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			panels. Authentication is not required to exploit this vulnerability. The specific flaw exists within the authentication mechanism. The issue is due to insufficient authentication on post-authentication requests. An attacker can leverage this vulnerability to escalate privileges to resources normally protected from unauthenticated users. Was ZDI-CAN-10182. **CVE ID : CVE-2020-10918**		
Weak Cryptography for Passwords	23-Jul-20	4.3	This vulnerability allows remote attackers to disclose sensitive information on affected installations of C-MORE HMI EA9 Firmware version 6.52 touch screen panels. Authentication is not required to exploit this vulnerability. The specific flaw exists within the handling of passwords. When transmitting passwords, the process encrypts them in a recoverable format using a hard-coded key. An attacker can leverage this vulnerability to disclose credentials, leading to further compromise. Was ZDI-CAN-10185. **CVE ID : CVE-2020-10919**	N/A	H-AUT-EA9--190820/1046
Missing	23-Jul-20	7.5	This vulnerability allows	N/A	H-AUT-EA9--

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Authentication for Critical Function			remote attackers to execute arbitrary code on affected installations of C-MORE HMI EA9 Firmware version 6.52 touch screen panels. Authentication is not required to exploit this vulnerability. The specific flaw exists within the control service, which listens on TCP port 9999 by default. The issue results from the lack of authentication prior to allowing alterations to the system configuration. An attacker can leverage this vulnerability to execute code in the context of the device. Was ZDI-CAN-10493. **CVE ID : CVE-2020-10920**		190820/1047
Missing Authentication for Critical Function	23-Jul-20	7.5	This vulnerability allows remote attackers to issue commands on affected installations of C-MORE HMI EA9 Firmware version 6.52 touch screen panels. Authentication is not required to exploit this vulnerability. The specific flaw exists within the EA-HTTP.exe process. The issue results from the lack of authentication prior to allowing alterations to the system configuration. An attacker can leverage this vulnerability to issue commands to the physical equipment controlled by	N/A	H-AUT-EA9--190820/1048

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			the device. Was ZDI-CAN-10482. **CVE ID : CVE-2020-10921**		
Improper Input Validation	23-Jul-20	5	This vulnerability allows remote attackers to create a denial-of-service condition on affected installations of C-MORE HMI EA9 Firmware version 6.52 touch screen panels. Authentication is not required to exploit this vulnerability. The specific flaw exists within the EA-HTTP.exe process. The issue results from the lack of proper input validation prior to further processing user requests. An attacker can leverage this vulnerability to create a denial-of-service condition on the system. Was ZDI-CAN-10527. **CVE ID : CVE-2020-10922**	N/A	H-AUT-EA9--190820/1049
ea9-t15cl-r					
Improper Authentication	23-Jul-20	5	This vulnerability allows remote attackers to bypass authentication on affected installations of C-MORE HMI EA9 Firmware version 6.52 touch screen panels. Authentication is not required to exploit this vulnerability. The specific flaw exists within the authentication mechanism. The issue is due to insufficient authentication on post-authentication	N/A	H-AUT-EA9--190820/1050

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			requests. An attacker can leverage this vulnerability to escalate privileges to resources normally protected from unauthenticated users. Was ZDI-CAN-10182. **CVE ID : CVE-2020-10918**		
Weak Cryptography for Passwords	23-Jul-20	4.3	This vulnerability allows remote attackers to disclose sensitive information on affected installations of C-MORE HMI EA9 Firmware version 6.52 touch screen panels. Authentication is not required to exploit this vulnerability. The specific flaw exists within the handling of passwords. When transmitting passwords, the process encrypts them in a recoverable format using a hard-coded key. An attacker can leverage this vulnerability to disclose credentials, leading to further compromise. Was ZDI-CAN-10185. **CVE ID : CVE-2020-10919**	N/A	H-AUT-EA9--190820/1051
Missing Authentication for Critical Function	23-Jul-20	7.5	This vulnerability allows remote attackers to execute arbitrary code on affected installations of C-MORE HMI EA9 Firmware version 6.52 touch screen panels. Authentication is not required to exploit this vulnerability. The specific	N/A	H-AUT-EA9--190820/1052

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			flaw exists within the control service, which listens on TCP port 9999 by default. The issue results from the lack of authentication prior to allowing alterations to the system configuration. An attacker can leverage this vulnerability to execute code in the context of the device. Was ZDI-CAN-10493. **CVE ID : CVE-2020-10920**		
Missing Authentication for Critical Function	23-Jul-20	7.5	This vulnerability allows remote attackers to issue commands on affected installations of C-MORE HMI EA9 Firmware version 6.52 touch screen panels. Authentication is not required to exploit this vulnerability. The specific flaw exists within the EA-HTTP.exe process. The issue results from the lack of authentication prior to allowing alterations to the system configuration. An attacker can leverage this vulnerability to issue commands to the physical equipment controlled by the device. Was ZDI-CAN-10482. **CVE ID : CVE-2020-10921**	N/A	H-AUT-EA9--190820/1053
Improper Input Validation	23-Jul-20	5	This vulnerability allows remote attackers to create a denial-of-service condition on affected	N/A	H-AUT-EA9--190820/1054

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			installations of C-MORE HMI EA9 Firmware version 6.52 touch screen panels. Authentication is not required to exploit this vulnerability. The specific flaw exists within the EA-HTTP.exe process. The issue results from the lack of proper input validation prior to further processing user requests. An attacker can leverage this vulnerability to create a denial-of-service condition on the system. Was ZDI-CAN-10527. **CVE ID : CVE-2020-10922**		
ea9-t6cl					
Improper Authentication	23-Jul-20	5	This vulnerability allows remote attackers to bypass authentication on affected installations of C-MORE HMI EA9 Firmware version 6.52 touch screen panels. Authentication is not required to exploit this vulnerability. The specific flaw exists within the authentication mechanism. The issue is due to insufficient authentication on post-authentication requests. An attacker can leverage this vulnerability to escalate privileges to resources normally protected from unauthenticated users. Was ZDI-CAN-10182.	N/A	H-AUT-EA9--190820/1055

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2020-10918		
Weak Cryptography for Passwords	23-Jul-20	4.3	This vulnerability allows remote attackers to disclose sensitive information on affected installations of C-MORE HMI EA9 Firmware version 6.52 touch screen panels. Authentication is not required to exploit this vulnerability. The specific flaw exists within the handling of passwords. When transmitting passwords, the process encrypts them in a recoverable format using a hard-coded key. An attacker can leverage this vulnerability to disclose credentials, leading to further compromise. Was ZDI-CAN-10185. **CVE ID : CVE-2020-10919**	N/A	H-AUT-EA9--190820/1056
Missing Authentication for Critical Function	23-Jul-20	7.5	This vulnerability allows remote attackers to execute arbitrary code on affected installations of C-MORE HMI EA9 Firmware version 6.52 touch screen panels. Authentication is not required to exploit this vulnerability. The specific flaw exists within the control service, which listens on TCP port 9999 by default. The issue results from the lack of authentication prior to allowing alterations to the	N/A	H-AUT-EA9--190820/1057

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			system configuration. An attacker can leverage this vulnerability to execute code in the context of the device. Was ZDI-CAN-10493. **CVE ID : CVE-2020-10920**		
Missing Authentication for Critical Function	23-Jul-20	7.5	This vulnerability allows remote attackers to issue commands on affected installations of C-MORE HMI EA9 Firmware version 6.52 touch screen panels. Authentication is not required to exploit this vulnerability. The specific flaw exists within the EA-HTTP.exe process. The issue results from the lack of authentication prior to allowing alterations to the system configuration. An attacker can leverage this vulnerability to issue commands to the physical equipment controlled by the device. Was ZDI-CAN-10482. **CVE ID : CVE-2020-10921**	N/A	H-AUT-EA9--190820/1058
Improper Input Validation	23-Jul-20	5	This vulnerability allows remote attackers to create a denial-of-service condition on affected installations of C-MORE HMI EA9 Firmware version 6.52 touch screen panels. Authentication is not required to exploit this vulnerability. The specific flaw exists within the EA-	N/A	H-AUT-EA9--190820/1059

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			HTTP.exe process. The issue results from the lack of proper input validation prior to further processing user requests. An attacker can leverage this vulnerability to create a denial-of-service condition on the system. Was ZDI-CAN-10527. **CVE ID : CVE-2020-10922**		
ea9-t6cl-r					
Improper Authentication	23-Jul-20	5	This vulnerability allows remote attackers to bypass authentication on affected installations of C-MORE HMI EA9 Firmware version 6.52 touch screen panels. Authentication is not required to exploit this vulnerability. The specific flaw exists within the authentication mechanism. The issue is due to insufficient authentication on post-authentication requests. An attacker can leverage this vulnerability to escalate privileges to resources normally protected from unauthenticated users. Was ZDI-CAN-10182. **CVE ID : CVE-2020-10918**	N/A	H-AUT-EA9--190820/1060
Weak Cryptography for Passwords	23-Jul-20	4.3	This vulnerability allows remote attackers to disclose sensitive information on affected installations of C-MORE HMI EA9 Firmware	N/A	H-AUT-EA9--190820/1061

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			version 6.52 touch screen panels. Authentication is not required to exploit this vulnerability. The specific flaw exists within the handling of passwords. When transmitting passwords, the process encrypts them in a recoverable format using a hard-coded key. An attacker can leverage this vulnerability to disclose credentials, leading to further compromise. Was ZDI-CAN-10185. **CVE ID : CVE-2020-10919**		
Missing Authenticati on for Critical Function	23-Jul-20	7.5	This vulnerability allows remote attackers to execute arbitrary code on affected installations of C-MORE HMI EA9 Firmware version 6.52 touch screen panels. Authentication is not required to exploit this vulnerability. The specific flaw exists within the control service, which listens on TCP port 9999 by default. The issue results from the lack of authentication prior to allowing alterations to the system configuration. An attacker can leverage this vulnerability to execute code in the context of the device. Was ZDI-CAN-10493. **CVE ID : CVE-2020-10920**	N/A	H-AUT-EA9--190820/1062

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Missing Authentication for Critical Function	23-Jul-20	7.5	This vulnerability allows remote attackers to issue commands on affected installations of C-MORE HMI EA9 Firmware version 6.52 touch screen panels. Authentication is not required to exploit this vulnerability. The specific flaw exists within the EA-HTTP.exe process. The issue results from the lack of authentication prior to allowing alterations to the system configuration. An attacker can leverage this vulnerability to issue commands to the physical equipment controlled by the device. Was ZDI-CAN-10482. **CVE ID : CVE-2020-10921**	N/A	H-AUT-EA9--190820/1063
Improper Input Validation	23-Jul-20	5	This vulnerability allows remote attackers to create a denial-of-service condition on affected installations of C-MORE HMI EA9 Firmware version 6.52 touch screen panels. Authentication is not required to exploit this vulnerability. The specific flaw exists within the EA-HTTP.exe process. The issue results from the lack of proper input validation prior to further processing user requests. An attacker can leverage this vulnerability to create a denial-of-service condition	N/A	H-AUT-EA9--190820/1064

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			on the system. Was ZDI-CAN-10527. **CVE ID : CVE-2020-10922**		
ea9-t7cl					
Improper Authenticati on	23-Jul-20	5	This vulnerability allows remote attackers to bypass authentication on affected installations of C-MORE HMI EA9 Firmware version 6.52 touch screen panels. Authentication is not required to exploit this vulnerability. The specific flaw exists within the authentication mechanism. The issue is due to insufficient authentication on post-authentication requests. An attacker can leverage this vulnerability to escalate privileges to resources normally protected from unauthenticated users. Was ZDI-CAN-10182. **CVE ID : CVE-2020-10918**	N/A	H-AUT-EA9--190820/1065
Weak Cryptograph y for Passwords	23-Jul-20	4.3	This vulnerability allows remote attackers to disclose sensitive information on affected installations of C-MORE HMI EA9 Firmware version 6.52 touch screen panels. Authentication is not required to exploit this vulnerability. The specific flaw exists within the handling of passwords. When transmitting passwords, the process	N/A	H-AUT-EA9--190820/1066

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			encrypts them in a recoverable format using a hard-coded key. An attacker can leverage this vulnerability to disclose credentials, leading to further compromise. Was ZDI-CAN-10185. **CVE ID : CVE-2020-10919**		
Missing Authenticati on for Critical Function	23-Jul-20	7.5	This vulnerability allows remote attackers to execute arbitrary code on affected installations of C-MORE HMI EA9 Firmware version 6.52 touch screen panels. Authentication is not required to exploit this vulnerability. The specific flaw exists within the control service, which listens on TCP port 9999 by default. The issue results from the lack of authentication prior to allowing alterations to the system configuration. An attacker can leverage this vulnerability to execute code in the context of the device. Was ZDI-CAN-10493. **CVE ID : CVE-2020-10920**	N/A	H-AUT-EA9--190820/1067
Missing Authenticati on for Critical Function	23-Jul-20	7.5	This vulnerability allows remote attackers to issue commands on affected installations of C-MORE HMI EA9 Firmware version 6.52 touch screen panels. Authentication is not required to exploit this	N/A	H-AUT-EA9--190820/1068

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			vulnerability. The specific flaw exists within the EA-HTTP.exe process. The issue results from the lack of authentication prior to allowing alterations to the system configuration. An attacker can leverage this vulnerability to issue commands to the physical equipment controlled by the device. Was ZDI-CAN-10482. **CVE ID : CVE-2020-10921**		
Improper Input Validation	23-Jul-20	5	This vulnerability allows remote attackers to create a denial-of-service condition on affected installations of C-MORE HMI EA9 Firmware version 6.52 touch screen panels. Authentication is not required to exploit this vulnerability. The specific flaw exists within the EA-HTTP.exe process. The issue results from the lack of proper input validation prior to further processing user requests. An attacker can leverage this vulnerability to create a denial-of-service condition on the system. Was ZDI-CAN-10527. **CVE ID : CVE-2020-10922**	N/A	H-AUT-EA9--190820/1069
ea9-t7cl-r					
Improper Authenticati	23-Jul-20	5	This vulnerability allows remote attackers to bypass authentication on affected	N/A	H-AUT-EA9--190820/1070

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
on			installations of C-MORE HMI EA9 Firmware version 6.52 touch screen panels. Authentication is not required to exploit this vulnerability. The specific flaw exists within the authentication mechanism. The issue is due to insufficient authentication on post-authentication requests. An attacker can leverage this vulnerability to escalate privileges to resources normally protected from unauthenticated users. Was ZDI-CAN-10182. **CVE ID : CVE-2020-10918**		
Weak Cryptography for Passwords	23-Jul-20	4.3	This vulnerability allows remote attackers to disclose sensitive information on affected installations of C-MORE HMI EA9 Firmware version 6.52 touch screen panels. Authentication is not required to exploit this vulnerability. The specific flaw exists within the handling of passwords. When transmitting passwords, the process encrypts them in a recoverable format using a hard-coded key. An attacker can leverage this vulnerability to disclose credentials, leading to further compromise. Was	N/A	H-AUT-EA9--190820/1071

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			ZDI-CAN-10185. **CVE ID : CVE-2020-10919**		
Missing Authenticati on for Critical Function	23-Jul-20	7.5	This vulnerability allows remote attackers to execute arbitrary code on affected installations of C-MORE HMI EA9 Firmware version 6.52 touch screen panels. Authentication is not required to exploit this vulnerability. The specific flaw exists within the control service, which listens on TCP port 9999 by default. The issue results from the lack of authentication prior to allowing alterations to the system configuration. An attacker can leverage this vulnerability to execute code in the context of the device. Was ZDI-CAN-10493. **CVE ID : CVE-2020-10920**	N/A	H-AUT-EA9--190820/1072
Missing Authenticati on for Critical Function	23-Jul-20	7.5	This vulnerability allows remote attackers to issue commands on affected installations of C-MORE HMI EA9 Firmware version 6.52 touch screen panels. Authentication is not required to exploit this vulnerability. The specific flaw exists within the EA-HTTP.exe process. The issue results from the lack of authentication prior to allowing alterations to the system configuration. An	N/A	H-AUT-EA9--190820/1073

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			attacker can leverage this vulnerability to issue commands to the physical equipment controlled by the device. Was ZDI-CAN-10482. **CVE ID : CVE-2020-10921**		
Improper Input Validation	23-Jul-20	5	This vulnerability allows remote attackers to create a denial-of-service condition on affected installations of C-MORE HMI EA9 Firmware version 6.52 touch screen panels. Authentication is not required to exploit this vulnerability. The specific flaw exists within the EA-HTTP.exe process. The issue results from the lack of proper input validation prior to further processing user requests. An attacker can leverage this vulnerability to create a denial-of-service condition on the system. Was ZDI-CAN-10527. **CVE ID : CVE-2020-10922**	N/A	H-AUT-EA9--190820/1074
ea9-t8cl					
Improper Authenticati on	23-Jul-20	5	This vulnerability allows remote attackers to bypass authentication on affected installations of C-MORE HMI EA9 Firmware version 6.52 touch screen panels. Authentication is not required to exploit this vulnerability. The specific flaw exists within the	N/A	H-AUT-EA9--190820/1075

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			authentication mechanism. The issue is due to insufficient authentication on post-authentication requests. An attacker can leverage this vulnerability to escalate privileges to resources normally protected from unauthenticated users. Was ZDI-CAN-10182. **CVE ID : CVE-2020-10918**		
Weak Cryptography for Passwords	23-Jul-20	4.3	This vulnerability allows remote attackers to disclose sensitive information on affected installations of C-MORE HMI EA9 Firmware version 6.52 touch screen panels. Authentication is not required to exploit this vulnerability. The specific flaw exists within the handling of passwords. When transmitting passwords, the process encrypts them in a recoverable format using a hard-coded key. An attacker can leverage this vulnerability to disclose credentials, leading to further compromise. Was ZDI-CAN-10185. **CVE ID : CVE-2020-10919**	N/A	H-AUT-EA9--190820/1076
Missing Authentication for Critical Function	23-Jul-20	7.5	This vulnerability allows remote attackers to execute arbitrary code on affected installations of C-MORE HMI EA9 Firmware	N/A	H-AUT-EA9--190820/1077

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			version 6.52 touch screen panels. Authentication is not required to exploit this vulnerability. The specific flaw exists within the control service, which listens on TCP port 9999 by default. The issue results from the lack of authentication prior to allowing alterations to the system configuration. An attacker can leverage this vulnerability to execute code in the context of the device. Was ZDI-CAN-10493. **CVE ID : CVE-2020-10920**		
Missing Authenticati on for Critical Function	23-Jul-20	7.5	This vulnerability allows remote attackers to issue commands on affected installations of C-MORE HMI EA9 Firmware version 6.52 touch screen panels. Authentication is not required to exploit this vulnerability. The specific flaw exists within the EA-HTTP.exe process. The issue results from the lack of authentication prior to allowing alterations to the system configuration. An attacker can leverage this vulnerability to issue commands to the physical equipment controlled by the device. Was ZDI-CAN-10482. **CVE ID : CVE-2020-10921**	N/A	H-AUT-EA9--190820/1078

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Improper Input Validation	23-Jul-20	5	This vulnerability allows remote attackers to create a denial-of-service condition on affected installations of C-MORE HMI EA9 Firmware version 6.52 touch screen panels. Authentication is not required to exploit this vulnerability. The specific flaw exists within the EA-HTTP.exe process. The issue results from the lack of proper input validation prior to further processing user requests. An attacker can leverage this vulnerability to create a denial-of-service condition on the system. Was ZDI-CAN-10527. **CVE ID : CVE-2020-10922**	N/A	H-AUT-EA9--190820/1079
avertx					
hd838					
N/A	23-Jul-20	7.2	An issue was discovered in AvertX Auto focus Night Vision HD Indoor/Outdoor IP Dome Camera HD838 and Night Vision HD Indoor/Outdoor Mini IP Bullet Camera HD438. An attacker with physical access to the UART interface could access additional diagnostic and configuration functionalities as well as the camera's bootloader. Successful exploitation could compromise	N/A	H-AVE-HD83-190820/1080

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			confidentiality, integrity, and availability of the affected system. It could even render the device inoperable. **CVE ID : CVE-2020-11623**		
Weak Password Requirements	23-Jul-20	7.5	An issue was discovered in AvertX Auto focus Night Vision HD Indoor/Outdoor IP Dome Camera HD838 and Night Vision HD Indoor/Outdoor Mini IP Bullet Camera HD438. They do not require users to change the default password for the admin account. They only show a pop-up window suggesting a change but there's no enforcement. An administrator can click Cancel and proceed to use the device without changing the password. Additionally, they disclose the default username within the login.js script. Since many attacks for IoT devices, including malware and exploits, are based on the usage of default credentials, it makes these cameras an easy target for malicious actors. **CVE ID : CVE-2020-11624**	N/A	H-AVE-HD83-190820/1081
Information Exposure Through Discrepancy	23-Jul-20	5	An issue was discovered in AvertX Auto focus Night Vision HD Indoor/Outdoor IP Dome Camera HD838 and Night Vision HD	N/A	H-AVE-HD83-190820/1082

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Indoor/Outdoor Mini IP Bullet Camera HD438. Failed web UI login attempts elicit different responses depending on whether a user account exists. Because the responses indicate whether a submitted username is valid or not, they make it easier to identify legitimate usernames. If a login request is sent to ISAPI/Security/sessionLogin/capabilities using a username that exists, it will return the value of the salt given to that username, even if the password is incorrect. However, if a login request is sent using a username that is not present in the database, it will return an empty salt value. This allows attackers to enumerate legitimate usernames, facilitating brute-force attacks. NOTE: this is different from CVE-2020-7057. **CVE ID : CVE-2020-11625**		
hd438					
N/A	23-Jul-20	7.2	An issue was discovered in AvertX Auto focus Night Vision HD Indoor/Outdoor IP Dome Camera HD838 and Night Vision HD Indoor/Outdoor Mini IP	N/A	H-AVE-HD43-190820/1083

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Bullet Camera HD438. An attacker with physical access to the UART interface could access additional diagnostic and configuration functionalities as well as the camera's bootloader. Successful exploitation could compromise confidentiality, integrity, and availability of the affected system. It could even render the device inoperable. **CVE ID : CVE-2020-11623**		
Weak Password Requirements	23-Jul-20	7.5	An issue was discovered in AvertX Auto focus Night Vision HD Indoor/Outdoor IP Dome Camera HD838 and Night Vision HD Indoor/Outdoor Mini IP Bullet Camera HD438. They do not require users to change the default password for the admin account. They only show a pop-up window suggesting a change but there's no enforcement. An administrator can click Cancel and proceed to use the device without changing the password. Additionally, they disclose the default username within the login.js script. Since many attacks for IoT devices, including malware and exploits, are based on the usage of default	N/A	H-AVE-HD43-190820/1084

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			credentials, it makes these cameras an easy target for malicious actors. **CVE ID : CVE-2020-11624**		
Information Exposure Through Discrepancy	23-Jul-20	5	An issue was discovered in AvertX Auto focus Night Vision HD Indoor/Outdoor IP Dome Camera HD838 and Night Vision HD Indoor/Outdoor Mini IP Bullet Camera HD438. Failed web UI login attempts elicit different responses depending on whether a user account exists. Because the responses indicate whether a submitted username is valid or not, they make it easier to identify legitimate usernames. If a login request is sent to ISAPI/Security/sessionLogin/capabilities using a username that exists, it will return the value of the salt given to that username, even if the password is incorrect. However, if a login request is sent using a username that is not present in the database, it will return an empty salt value. This allows attackers to enumerate legitimate usernames, facilitating brute-force attacks. NOTE: this is different from CVE-	N/A	H-AVE-HD43-190820/1085

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			2020-7057. **CVE ID : CVE-2020-11625**		
Cisco					
asa_5540					
Improper Input Validation	22-Jul-20	5	A vulnerability in the web services interface of Cisco Adaptive Security Appliance (ASA) Software and Cisco Firepower Threat Defense (FTD) Software could allow an unauthenticated, remote attacker to conduct directory traversal attacks and read sensitive files on a targeted system. The vulnerability is due to a lack of proper input validation of URLs in HTTP requests processed by an affected device. An attacker could exploit this vulnerability by sending a crafted HTTP request containing directory traversal character sequences to an affected device. A successful exploit could allow the attacker to view arbitrary files within the web services file system on the targeted device. The web services file system is enabled when the affected device is configured with either WebVPN or AnyConnect features. This vulnerability cannot be used to obtain access to ASA or FTD	N/A	H-CIS-ASA_-190820/1086

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			system files or underlying operating system (OS) files. **CVE ID : CVE-2020-3452**		
rv110w					
Incorrect Authorization	16-Jul-20	4.3	A vulnerability in the web-based management interface of Cisco Small Business RV110W and RV215W Series Routers could allow an unauthenticated, remote attacker to download sensitive information from the device, which could include the device configuration. The vulnerability is due to improper authorization of an HTTP request. An attacker could exploit this vulnerability by accessing a specific URI on the web-based management interface of the router, but only after any valid user has opened a specific file on the device since the last reboot. A successful exploit would allow the attacker to view sensitive information, which should be restricted. **CVE ID : CVE-2020-3150**	N/A	H-CIS-RV11-190820/1087
Improper Authentication	16-Jul-20	7.5	A vulnerability in the web-based management interface of the Cisco RV110W Wireless-N VPN Firewall, RV130 VPN Router, RV130W Wireless-	N/A	H-CIS-RV11-190820/1088

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			N Multifunction VPN Router, and RV215W Wireless-N VPN Router could allow an unauthenticated, remote attacker to bypass authentication and execute arbitrary commands with administrative commands on an affected device. The vulnerability is due to improper session management on affected devices. An attacker could exploit this vulnerability by sending a crafted HTTP request to the affected device. A successful exploit could allow the attacker to gain administrative access on the affected device. **CVE ID : CVE-2020-3144**		
Improper Restriction of Operations within the Bounds of a Memory Buffer	16-Jul-20	6.5	Multiple vulnerabilities in the web-based management interface of the Cisco RV110W Wireless-N VPN Firewall, RV130 VPN Router, RV130W Wireless-N Multifunction VPN Router, and RV215W Wireless-N VPN Router could allow an authenticated, remote attacker to execute arbitrary code on an affected device. The vulnerabilities are due to improper validation of user-supplied data in the web-based management interface. An attacker	N/A	H-CIS-RV11-190820/1089

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			could exploit these vulnerabilities by sending malicious HTTP requests to a targeted device. A successful exploit could allow the attacker to execute arbitrary code on the underlying operating system of the affected device as a high-privilege user. **CVE ID : CVE-2020-3145**		
rv130w					
Improper Authentication	16-Jul-20	7.5	A vulnerability in the web-based management interface of the Cisco RV110W Wireless-N VPN Firewall, RV130 VPN Router, RV130W Wireless-N Multifunction VPN Router, and RV215W Wireless-N VPN Router could allow an unauthenticated, remote attacker to bypass authentication and execute arbitrary commands with administrative commands on an affected device. The vulnerability is due to improper session management on affected devices. An attacker could exploit this vulnerability by sending a crafted HTTP request to the affected device. A successful exploit could allow the attacker to gain administrative access on the affected device.	N/A	H-CIS-RV13-190820/1090

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2020-3144		
Improper Restriction of Operations within the Bounds of a Memory Buffer	16-Jul-20	6.5	Multiple vulnerabilities in the web-based management interface of the Cisco RV110W Wireless-N VPN Firewall, RV130 VPN Router, RV130W Wireless-N Multifunction VPN Router, and RV215W Wireless-N VPN Router could allow an authenticated, remote attacker to execute arbitrary code on an affected device. The vulnerabilities are due to improper validation of user-supplied data in the web-based management interface. An attacker could exploit these vulnerabilities by sending malicious HTTP requests to a targeted device. A successful exploit could allow the attacker to execute arbitrary code on the underlying operating system of the affected device as a high-privilege user. **CVE ID : CVE-2020-3145**	N/A	H-CIS-RV13-190820/1091
Improper Restriction of Operations within the Bounds of a Memory Buffer	16-Jul-20	9	Multiple vulnerabilities in the web-based management interface of the Cisco RV110W Wireless-N VPN Firewall, RV130 VPN Router, RV130W Wireless-N Multifunction VPN Router,	N/A	H-CIS-RV13-190820/1092

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			and RV215W Wireless-N VPN Router could allow an authenticated, remote attacker to execute arbitrary code on an affected device. The vulnerabilities are due to improper validation of user-supplied data in the web-based management interface. An attacker could exploit these vulnerabilities by sending malicious HTTP requests to a targeted device. A successful exploit could allow the attacker to execute arbitrary code on the underlying operating system of the affected device as a high-privilege user. **CVE ID : CVE-2020-3146**		
rv215w					
Incorrect Authorizatio n	16-Jul-20	4.3	A vulnerability in the web-based management interface of Cisco Small Business RV110W and RV215W Series Routers could allow an unauthenticated, remote attacker to download sensitive information from the device, which could include the device configuration. The vulnerability is due to improper authorization of an HTTP request. An attacker could exploit this	N/A	H-CIS-RV21-190820/1093

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			vulnerability by accessing a specific URI on the web-based management interface of the router, but only after any valid user has opened a specific file on the device since the last reboot. A successful exploit would allow the attacker to view sensitive information, which should be restricted. **CVE ID : CVE-2020-3150**		
Improper Authenticati on	16-Jul-20	7.5	A vulnerability in the web-based management interface of the Cisco RV110W Wireless-N VPN Firewall, RV130 VPN Router, RV130W Wireless-N Multifunction VPN Router, and RV215W Wireless-N VPN Router could allow an unauthenticated, remote attacker to bypass authentication and execute arbitrary commands with administrative commands on an affected device. The vulnerability is due to improper session management on affected devices. An attacker could exploit this vulnerability by sending a crafted HTTP request to the affected device. A successful exploit could allow the attacker to gain administrative access on the affected device.	N/A	H-CIS-RV21-190820/1094

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2020-3144		
Improper Restriction of Operations within the Bounds of a Memory Buffer	16-Jul-20	6.5	Multiple vulnerabilities in the web-based management interface of the Cisco RV110W Wireless-N VPN Firewall, RV130 VPN Router, RV130W Wireless-N Multifunction VPN Router, and RV215W Wireless-N VPN Router could allow an authenticated, remote attacker to execute arbitrary code on an affected device. The vulnerabilities are due to improper validation of user-supplied data in the web-based management interface. An attacker could exploit these vulnerabilities by sending malicious HTTP requests to a targeted device. A successful exploit could allow the attacker to execute arbitrary code on the underlying operating system of the affected device as a high-privilege user. **CVE ID : CVE-2020-3145**	N/A	H-CIS-RV21-190820/1095
Improper Restriction of Operations within the Bounds of a Memory Buffer	16-Jul-20	9	Multiple vulnerabilities in the web-based management interface of the Cisco RV110W Wireless-N VPN Firewall, RV130 VPN Router, RV130W Wireless-N Multifunction VPN Router,	N/A	H-CIS-RV21-190820/1096

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			and RV215W Wireless-N VPN Router could allow an authenticated, remote attacker to execute arbitrary code on an affected device. The vulnerabilities are due to improper validation of user-supplied data in the web-based management interface. An attacker could exploit these vulnerabilities by sending malicious HTTP requests to a targeted device. A successful exploit could allow the attacker to execute arbitrary code on the underlying operating system of the affected device as a high-privilege user. **CVE ID : CVE-2020-3146**		
isr1100-4g					
Insufficiently Protected Credentials	16-Jul-20	7.2	A vulnerability in Cisco SD-WAN Solution Software could allow an unauthenticated, local attacker to access an affected device by using an account that has a default, static password. This account has root privileges. The vulnerability exists because the affected software has a user account with a default, static password. An attacker could exploit this	N/A	H-CIS-ISR1-190820/1097

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			vulnerability by remotely connecting to an affected system by using this account. A successful exploit could allow the attacker to log in by using this account with root privileges. **CVE ID : CVE-2020-3180**		
Uncontrolled Resource Consumption	16-Jul-20	4	A vulnerability in the web-based management interface of Cisco SD-WAN vManage Software could allow an authenticated, remote attacker to consume excessive system memory and cause a denial of service (DoS) condition on an affected system. The vulnerability is due to inefficient memory management. An attacker could exploit this vulnerability by sending a large number of crafted HTTP requests to the affected web-based management interface. A successful exploit could allow the attacker to exhaust system memory, which could cause the system to stop processing new connections and could result in a DoS condition. **CVE ID : CVE-2020-3372**	N/A	H-CIS-ISR1-190820/1098
Improper Neutralization of Special Elements	16-Jul-20	4	A vulnerability in the web-based management interface for Cisco SD-WAN vManage Software	N/A	H-CIS-ISR1-190820/1099

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
used in an SQL Command ('SQL Injection')			could allow an authenticated, remote attacker to impact the integrity of an affected system by executing arbitrary SQL queries. The vulnerability is due to insufficient validation of user-supplied input. An attacker could exploit this vulnerability by sending crafted input that includes SQL statements to an affected system. A successful exploit could allow the attacker to modify entries in some database tables, affecting the integrity of the data. **CVE ID : CVE-2020-3378**		
Improper Limitation of a Pathname to a Restricted Directory ('Path Traversal')	16-Jul-20	6.5	A vulnerability in the web management interface of Cisco SD-WAN vManage Software could allow an authenticated, remote attacker to conduct directory traversal attacks and obtain read and write access to sensitive files on a targeted system. The vulnerability is due to a lack of proper validation of files that are uploaded to an affected device. An attacker could exploit this vulnerability by uploading a crafted file to an affected system. An exploit could allow the attacker to view or modify arbitrary files on	N/A	H-CIS-ISR1-190820/1100

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			the targeted system. **CVE ID : CVE-2020-3381**		
Improper Input Validation	16-Jul-20	9	A vulnerability in Cisco SD-WAN vManage Software could allow an authenticated, remote attacker to execute code with root privileges on an affected system. The vulnerability is due to insufficient input sanitization during user authentication processing. An attacker could exploit this vulnerability by sending a crafted response to the Cisco SD-WAN vManage Software. A successful exploit could allow the attacker to access the software and execute commands they should not be authorized to execute. **CVE ID : CVE-2020-3387**	N/A	H-CIS-ISR1-190820/1101
Improper Authenticati on	16-Jul-20	7.2	A vulnerability in the CLI of Cisco SD-WAN vManage Software could allow an authenticated, local attacker to inject arbitrary commands that are executed with root privileges. The vulnerability is due to insufficient input validation. An attacker could exploit this vulnerability by authenticating to the device and submitting	N/A	H-CIS-ISR1-190820/1102

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			crafted input to the CLI. The attacker must be authenticated to access the CLI. A successful exploit could allow the attacker to execute commands with root privileges. **CVE ID : CVE-2020-3388**		
Improper Limitation of a Pathname to a Restricted Directory ('Path Traversal')	16-Jul-20	4	A vulnerability in the web-based management interface of Cisco SD-WAN vManage Software could allow an authenticated, remote attacker to conduct path traversal attacks and obtain read access to sensitive files on an affected system. The vulnerability is due to insufficient validation of HTTP requests. An attacker could exploit this vulnerability by sending a crafted HTTP request that contains directory traversal character sequences to the affected system. A successful exploit could allow the attacker to view arbitrary files on the affected system. **CVE ID : CVE-2020-3401**	N/A	H-CIS-ISR1-190820/1103
rv130					
Improper Authenticati on	16-Jul-20	7.5	A vulnerability in the web-based management interface of the Cisco RV110W Wireless-N VPN Firewall, RV130 VPN Router, RV130W Wireless-	N/A	H-CIS-RV13-190820/1104

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			N Multifunction VPN Router, and RV215W Wireless-N VPN Router could allow an unauthenticated, remote attacker to bypass authentication and execute arbitrary commands with administrative commands on an affected device. The vulnerability is due to improper session management on affected devices. An attacker could exploit this vulnerability by sending a crafted HTTP request to the affected device. A successful exploit could allow the attacker to gain administrative access on the affected device. **CVE ID : CVE-2020-3144**		
Improper Restriction of Operations within the Bounds of a Memory Buffer	16-Jul-20	6.5	Multiple vulnerabilities in the web-based management interface of the Cisco RV110W Wireless-N VPN Firewall, RV130 VPN Router, RV130W Wireless-N Multifunction VPN Router, and RV215W Wireless-N VPN Router could allow an authenticated, remote attacker to execute arbitrary code on an affected device. The vulnerabilities are due to improper validation of user-supplied data in the web-based management interface. An attacker	N/A	H-CIS-RV13-190820/1105

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			could exploit these vulnerabilities by sending malicious HTTP requests to a targeted device. A successful exploit could allow the attacker to execute arbitrary code on the underlying operating system of the affected device as a high-privilege user. **CVE ID : CVE-2020-3145**		
Improper Restriction of Operations within the Bounds of a Memory Buffer	16-Jul-20	9	Multiple vulnerabilities in the web-based management interface of the Cisco RV110W Wireless-N VPN Firewall, RV130 VPN Router, RV130W Wireless-N Multifunction VPN Router, and RV215W Wireless-N VPN Router could allow an authenticated, remote attacker to execute arbitrary code on an affected device. The vulnerabilities are due to improper validation of user-supplied data in the web-based management interface. An attacker could exploit these vulnerabilities by sending malicious HTTP requests to a targeted device. A successful exploit could allow the attacker to execute arbitrary code on the underlying operating system of the affected device as a high-privilege	N/A	H-CIS-RV13-190820/1106

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			user. **CVE ID : CVE-2020-3146**		
asa_5545-x					
Improper Input Validation	22-Jul-20	5	A vulnerability in the web services interface of Cisco Adaptive Security Appliance (ASA) Software and Cisco Firepower Threat Defense (FTD) Software could allow an unauthenticated, remote attacker to conduct directory traversal attacks and read sensitive files on a targeted system. The vulnerability is due to a lack of proper input validation of URLs in HTTP requests processed by an affected device. An attacker could exploit this vulnerability by sending a crafted HTTP request containing directory traversal character sequences to an affected device. A successful exploit could allow the attacker to view arbitrary files within the web services file system on the targeted device. The web services file system is enabled when the affected device is configured with either WebVPN or AnyConnect features. This vulnerability cannot be used to obtain access to ASA or FTD system files or underlying	N/A	H-CIS-ASA_-190820/1107

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			operating system (OS) files. **CVE ID : CVE-2020-3452**		
vedge_100					
Insufficiently Protected Credentials	16-Jul-20	7.2	A vulnerability in Cisco SD-WAN Solution Software could allow an unauthenticated, local attacker to access an affected device by using an account that has a default, static password. This account has root privileges. The vulnerability exists because the affected software has a user account with a default, static password. An attacker could exploit this vulnerability by remotely connecting to an affected system by using this account. A successful exploit could allow the attacker to log in by using this account with root privileges. **CVE ID : CVE-2020-3180**	N/A	H-CIS-VEDG-190820/1108
Uncontrolled Resource Consumption	16-Jul-20	7.8	A vulnerability in Cisco SD-WAN Solution Software could allow an unauthenticated, remote attacker to cause a denial of service (DoS) condition. The vulnerability is due to improper validation of fields in Cisco SD-WAN peering messages that are encapsulated in UDP	N/A	H-CIS-VEDG-190820/1109

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			packets. An attacker could exploit this vulnerability by sending crafted UDP messages to the targeted system. A successful exploit could allow the attacker to cause services on the device to fail, resulting in a DoS condition that could impact the targeted device and other devices that depend on it. **CVE ID : CVE-2020-3351**		
Uncontrolled Resource Consumption	16-Jul-20	4	A vulnerability in the web-based management interface of Cisco SD-WAN vManage Software could allow an authenticated, remote attacker to consume excessive system memory and cause a denial of service (DoS) condition on an affected system. The vulnerability is due to inefficient memory management. An attacker could exploit this vulnerability by sending a large number of crafted HTTP requests to the affected web-based management interface. A successful exploit could allow the attacker to exhaust system memory, which could cause the system to stop processing new connections and could result in a DoS condition.	N/A	H-CIS-VEDG-190820/1110

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2020-3372		
Improper Neutralization of Special Elements used in an SQL Command ('SQL Injection')	16-Jul-20	4	A vulnerability in the web-based management interface for Cisco SD-WAN vManage Software could allow an authenticated, remote attacker to impact the integrity of an affected system by executing arbitrary SQL queries. The vulnerability is due to insufficient validation of user-supplied input. An attacker could exploit this vulnerability by sending crafted input that includes SQL statements to an affected system. A successful exploit could allow the attacker to modify entries in some database tables, affecting the integrity of the data. **CVE ID : CVE-2020-3378**	N/A	H-CIS-VEDG-190820/1111
Improper Input Validation	16-Jul-20	7.2	A vulnerability in Cisco SD-WAN Solution Software could allow an authenticated, local attacker to elevate privileges to Administrator on the underlying operating system. The vulnerability is due to insufficient input validation. An attacker could exploit this vulnerability by sending a crafted request to an affected system. A	N/A	H-CIS-VEDG-190820/1112

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			successful exploit could allow the attacker to gain administrative privileges. **CVE ID : CVE-2020-3379**		
Improper Limitation of a Pathname to a Restricted Directory ('Path Traversal')	16-Jul-20	4	A vulnerability in the web-based management interface of Cisco SD-WAN vManage Software could allow an authenticated, remote attacker to conduct path traversal attacks and obtain read access to sensitive files on an affected system. The vulnerability is due to insufficient validation of HTTP requests. An attacker could exploit this vulnerability by sending a crafted HTTP request that contains directory traversal character sequences to the affected system. A successful exploit could allow the attacker to view arbitrary files on the affected system. **CVE ID : CVE-2020-3401**	N/A	H-CIS-VEDG-190820/1113
vedge_1000					
Insufficiently Protected Credentials	16-Jul-20	7.2	A vulnerability in Cisco SD-WAN Solution Software could allow an unauthenticated, local attacker to access an affected device by using an account that has a default, static password. This account has root privileges. The	N/A	H-CIS-VEDG-190820/1114

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			vulnerability exists because the affected software has a user account with a default, static password. An attacker could exploit this vulnerability by remotely connecting to an affected system by using this account. A successful exploit could allow the attacker to log in by using this account with root privileges. **CVE ID : CVE-2020-3180**		
Uncontrolled Resource Consumption	16-Jul-20	7.8	A vulnerability in Cisco SD-WAN Solution Software could allow an unauthenticated, remote attacker to cause a denial of service (DoS) condition. The vulnerability is due to improper validation of fields in Cisco SD-WAN peering messages that are encapsulated in UDP packets. An attacker could exploit this vulnerability by sending crafted UDP messages to the targeted system. A successful exploit could allow the attacker to cause services on the device to fail, resulting in a DoS condition that could impact the targeted device and other devices that depend on it. **CVE ID : CVE-2020-3351**	N/A	H-CIS-VEDG-190820/1115

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Uncontrolled Resource Consumption	16-Jul-20	4	A vulnerability in the web-based management interface of Cisco SD-WAN vManage Software could allow an authenticated, remote attacker to consume excessive system memory and cause a denial of service (DoS) condition on an affected system. The vulnerability is due to inefficient memory management. An attacker could exploit this vulnerability by sending a large number of crafted HTTP requests to the affected web-based management interface. A successful exploit could allow the attacker to exhaust system memory, which could cause the system to stop processing new connections and could result in a DoS condition. **CVE ID : CVE-2020-3372**	N/A	H-CIS-VEDG-190820/1116
Improper Neutralization of Special Elements used in an SQL Command ('SQL Injection')	16-Jul-20	4	A vulnerability in the web-based management interface for Cisco SD-WAN vManage Software could allow an authenticated, remote attacker to impact the integrity of an affected system by executing arbitrary SQL queries. The vulnerability is due to insufficient validation of user-supplied input. An attacker could exploit this	N/A	H-CIS-VEDG-190820/1117

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			vulnerability by sending crafted input that includes SQL statements to an affected system. A successful exploit could allow the attacker to modify entries in some database tables, affecting the integrity of the data. **CVE ID : CVE-2020-3378**		
Improper Input Validation	16-Jul-20	7.2	A vulnerability in Cisco SD-WAN Solution Software could allow an authenticated, local attacker to elevate privileges to Administrator on the underlying operating system. The vulnerability is due to insufficient input validation. An attacker could exploit this vulnerability by sending a crafted request to an affected system. A successful exploit could allow the attacker to gain administrative privileges. **CVE ID : CVE-2020-3379**	N/A	H-CIS-VEDG-190820/1118
Improper Limitation of a Pathname to a Restricted Directory ('Path Traversal')	16-Jul-20	4	A vulnerability in the web-based management interface of Cisco SD-WAN vManage Software could allow an authenticated, remote attacker to conduct path traversal attacks and obtain read access to sensitive files on an affected system. The vulnerability is due to	N/A	H-CIS-VEDG-190820/1119

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			insufficient validation of HTTP requests. An attacker could exploit this vulnerability by sending a crafted HTTP request that contains directory traversal character sequences to the affected system. A successful exploit could allow the attacker to view arbitrary files on the affected system. **CVE ID : CVE-2020-3401**		
vedge_2000					
Insufficiently Protected Credentials	16-Jul-20	7.2	A vulnerability in Cisco SD-WAN Solution Software could allow an unauthenticated, local attacker to access an affected device by using an account that has a default, static password. This account has root privileges. The vulnerability exists because the affected software has a user account with a default, static password. An attacker could exploit this vulnerability by remotely connecting to an affected system by using this account. A successful exploit could allow the attacker to log in by using this account with root privileges. **CVE ID : CVE-2020-3180**	N/A	H-CIS-VEDG-190820/1120

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Uncontrolled Resource Consumption	16-Jul-20	7.8	A vulnerability in Cisco SD-WAN Solution Software could allow an unauthenticated, remote attacker to cause a denial of service (DoS) condition. The vulnerability is due to improper validation of fields in Cisco SD-WAN peering messages that are encapsulated in UDP packets. An attacker could exploit this vulnerability by sending crafted UDP messages to the targeted system. A successful exploit could allow the attacker to cause services on the device to fail, resulting in a DoS condition that could impact the targeted device and other devices that depend on it. **CVE ID : CVE-2020-3351**	N/A	H-CIS-VEDG-190820/1121
Uncontrolled Resource Consumption	16-Jul-20	4	A vulnerability in the web-based management interface of Cisco SD-WAN vManage Software could allow an authenticated, remote attacker to consume excessive system memory and cause a denial of service (DoS) condition on an affected system. The vulnerability is due to inefficient memory management. An attacker could exploit this vulnerability by sending a large number of crafted	N/A	H-CIS-VEDG-190820/1122

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			HTTP requests to the affected web-based management interface. A successful exploit could allow the attacker to exhaust system memory, which could cause the system to stop processing new connections and could result in a DoS condition. **CVE ID : CVE-2020-3372**		
Improper Neutralization of Special Elements used in an SQL Command ('SQL Injection')	16-Jul-20	4	A vulnerability in the web-based management interface for Cisco SD-WAN vManage Software could allow an authenticated, remote attacker to impact the integrity of an affected system by executing arbitrary SQL queries. The vulnerability is due to insufficient validation of user-supplied input. An attacker could exploit this vulnerability by sending crafted input that includes SQL statements to an affected system. A successful exploit could allow the attacker to modify entries in some database tables, affecting the integrity of the data. **CVE ID : CVE-2020-3378**	N/A	H-CIS-VEDG-190820/1123
Improper Input Validation	16-Jul-20	7.2	A vulnerability in Cisco SD-WAN Solution Software could allow an authenticated, local attacker to elevate	N/A	H-CIS-VEDG-190820/1124

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			privileges to Administrator on the underlying operating system. The vulnerability is due to insufficient input validation. An attacker could exploit this vulnerability by sending a crafted request to an affected system. A successful exploit could allow the attacker to gain administrative privileges. **CVE ID : CVE-2020-3379**		
Improper Limitation of a Pathname to a Restricted Directory ('Path Traversal')	16-Jul-20	4	A vulnerability in the web-based management interface of Cisco SD-WAN vManage Software could allow an authenticated, remote attacker to conduct path traversal attacks and obtain read access to sensitive files on an affected system. The vulnerability is due to insufficient validation of HTTP requests. An attacker could exploit this vulnerability by sending a crafted HTTP request that contains directory traversal character sequences to the affected system. A successful exploit could allow the attacker to view arbitrary files on the affected system. **CVE ID : CVE-2020-3401**	N/A	H-CIS-VEDG-190820/1125
vedge_5000					

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Insufficiently Protected Credentials	16-Jul-20	7.2	A vulnerability in Cisco SD-WAN Solution Software could allow an unauthenticated, local attacker to access an affected device by using an account that has a default, static password. This account has root privileges. The vulnerability exists because the affected software has a user account with a default, static password. An attacker could exploit this vulnerability by remotely connecting to an affected system by using this account. A successful exploit could allow the attacker to log in by using this account with root privileges. **CVE ID : CVE-2020-3180**	N/A	H-CIS-VEDG-190820/1126
Uncontrolled Resource Consumption	16-Jul-20	7.8	A vulnerability in Cisco SD-WAN Solution Software could allow an unauthenticated, remote attacker to cause a denial of service (DoS) condition. The vulnerability is due to improper validation of fields in Cisco SD-WAN peering messages that are encapsulated in UDP packets. An attacker could exploit this vulnerability by sending crafted UDP messages to the targeted system. A successful	N/A	H-CIS-VEDG-190820/1127

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			exploit could allow the attacker to cause services on the device to fail, resulting in a DoS condition that could impact the targeted device and other devices that depend on it. **CVE ID : CVE-2020-3351**		
N/A	16-Jul-20	7.8	A vulnerability in the deep packet inspection (DPI) engine of Cisco SD-WAN vEdge Routers could allow an unauthenticated, remote attacker to cause a denial of service (DoS) condition on an affected device. The vulnerability is due to improper processing of FTP traffic. An attacker could exploit this vulnerability by sending crafted FTP packets through an affected device. A successful exploit could allow the attacker to make the device reboot continuously, causing a DoS condition. **CVE ID : CVE-2020-3369**	N/A	H-CIS-VEDG-190820/1128
Uncontrolled Resource Consumption	16-Jul-20	4	A vulnerability in the web-based management interface of Cisco SD-WAN vManage Software could allow an authenticated, remote attacker to consume excessive system memory and cause a denial of service (DoS)	N/A	H-CIS-VEDG-190820/1129

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			condition on an affected system. The vulnerability is due to inefficient memory management. An attacker could exploit this vulnerability by sending a large number of crafted HTTP requests to the affected web-based management interface. A successful exploit could allow the attacker to exhaust system memory, which could cause the system to stop processing new connections and could result in a DoS condition. **CVE ID : CVE-2020-3372**		
Improper Neutralization of Special Elements used in an SQL Command ('SQL Injection')	16-Jul-20	4	A vulnerability in the web-based management interface for Cisco SD-WAN vManage Software could allow an authenticated, remote attacker to impact the integrity of an affected system by executing arbitrary SQL queries. The vulnerability is due to insufficient validation of user-supplied input. An attacker could exploit this vulnerability by sending crafted input that includes SQL statements to an affected system. A successful exploit could allow the attacker to modify entries in some database tables, affecting	N/A	H-CIS-VEDG-190820/1130

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			the integrity of the data. **CVE ID : CVE-2020-3378**		
Improper Input Validation	16-Jul-20	7.2	A vulnerability in Cisco SD-WAN Solution Software could allow an authenticated, local attacker to elevate privileges to Administrator on the underlying operating system. The vulnerability is due to insufficient input validation. An attacker could exploit this vulnerability by sending a crafted request to an affected system. A successful exploit could allow the attacker to gain administrative privileges. **CVE ID : CVE-2020-3379**	N/A	H-CIS-VEDG-190820/1131
N/A	16-Jul-20	6.1	A vulnerability in the deep packet inspection (DPI) engine of Cisco SD-WAN vEdge Routers could allow an unauthenticated, adjacent attacker to cause a denial of service (DoS) condition on an affected system. The vulnerability is due to insufficient handling of malformed packets. An attacker could exploit this vulnerability by sending crafted packets through an affected device. A successful exploit could allow the attacker to cause the device to reboot, resulting in a DoS	N/A	H-CIS-VEDG-190820/1132

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			condition. **CVE ID : CVE-2020-3385**		
Improper Limitation of a Pathname to a Restricted Directory ('Path Traversal')	16-Jul-20	4	A vulnerability in the web-based management interface of Cisco SD-WAN vManage Software could allow an authenticated, remote attacker to conduct path traversal attacks and obtain read access to sensitive files on an affected system. The vulnerability is due to insufficient validation of HTTP requests. An attacker could exploit this vulnerability by sending a crafted HTTP request that contains directory traversal character sequences to the affected system. A successful exploit could allow the attacker to view arbitrary files on the affected system. **CVE ID : CVE-2020-3401**	N/A	H-CIS-VEDG-190820/1133
vedge_100m					
Insufficiently Protected Credentials	16-Jul-20	7.2	A vulnerability in Cisco SD-WAN Solution Software could allow an unauthenticated, local attacker to access an affected device by using an account that has a default, static password. This account has root privileges. The vulnerability exists because the affected	N/A	H-CIS-VEDG-190820/1134

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			software has a user account with a default, static password. An attacker could exploit this vulnerability by remotely connecting to an affected system by using this account. A successful exploit could allow the attacker to log in by using this account with root privileges. **CVE ID : CVE-2020-3180**		
Uncontrolled Resource Consumption	16-Jul-20	7.8	A vulnerability in Cisco SD-WAN Solution Software could allow an unauthenticated, remote attacker to cause a denial of service (DoS) condition. The vulnerability is due to improper validation of fields in Cisco SD-WAN peering messages that are encapsulated in UDP packets. An attacker could exploit this vulnerability by sending crafted UDP messages to the targeted system. A successful exploit could allow the attacker to cause services on the device to fail, resulting in a DoS condition that could impact the targeted device and other devices that depend on it. **CVE ID : CVE-2020-3351**	N/A	H-CIS-VEDG-190820/1135
Uncontrolled Resource	16-Jul-20	4	A vulnerability in the web-based management	N/A	H-CIS-VEDG-190820/1136

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Consumption			interface of Cisco SD-WAN vManage Software could allow an authenticated, remote attacker to consume excessive system memory and cause a denial of service (DoS) condition on an affected system. The vulnerability is due to inefficient memory management. An attacker could exploit this vulnerability by sending a large number of crafted HTTP requests to the affected web-based management interface. A successful exploit could allow the attacker to exhaust system memory, which could cause the system to stop processing new connections and could result in a DoS condition. **CVE ID : CVE-2020-3372**		
Improper Neutralization of Special Elements used in an SQL Command ('SQL Injection')	16-Jul-20	4	A vulnerability in the web-based management interface for Cisco SD-WAN vManage Software could allow an authenticated, remote attacker to impact the integrity of an affected system by executing arbitrary SQL queries. The vulnerability is due to insufficient validation of user-supplied input. An attacker could exploit this vulnerability by sending crafted input that includes	N/A	H-CIS-VEDG-190820/1137

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			SQL statements to an affected system. A successful exploit could allow the attacker to modify entries in some database tables, affecting the integrity of the data. **CVE ID : CVE-2020-3378**		
Improper Input Validation	16-Jul-20	7.2	A vulnerability in Cisco SD-WAN Solution Software could allow an authenticated, local attacker to elevate privileges to Administrator on the underlying operating system. The vulnerability is due to insufficient input validation. An attacker could exploit this vulnerability by sending a crafted request to an affected system. A successful exploit could allow the attacker to gain administrative privileges. **CVE ID : CVE-2020-3379**	N/A	H-CIS-VEDG-190820/1138
Improper Limitation of a Pathname to a Restricted Directory ('Path Traversal')	16-Jul-20	4	A vulnerability in the web-based management interface of Cisco SD-WAN vManage Software could allow an authenticated, remote attacker to conduct path traversal attacks and obtain read access to sensitive files on an affected system. The vulnerability is due to insufficient validation of HTTP requests. An	N/A	H-CIS-VEDG-190820/1139

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			attacker could exploit this vulnerability by sending a crafted HTTP request that contains directory traversal character sequences to the affected system. A successful exploit could allow the attacker to view arbitrary files on the affected system. **CVE ID : CVE-2020-3401**		
vedge_100wm					
Insufficiently Protected Credentials	16-Jul-20	7.2	A vulnerability in Cisco SD-WAN Solution Software could allow an unauthenticated, local attacker to access an affected device by using an account that has a default, static password. This account has root privileges. The vulnerability exists because the affected software has a user account with a default, static password. An attacker could exploit this vulnerability by remotely connecting to an affected system by using this account. A successful exploit could allow the attacker to log in by using this account with root privileges. **CVE ID : CVE-2020-3180**	N/A	H-CIS-VEDG-190820/1140
Uncontrolled Resource	16-Jul-20	7.8	A vulnerability in Cisco SD-WAN Solution Software	N/A	H-CIS-VEDG-

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Consumption			could allow an unauthenticated, remote attacker to cause a denial of service (DoS) condition. The vulnerability is due to improper validation of fields in Cisco SD-WAN peering messages that are encapsulated in UDP packets. An attacker could exploit this vulnerability by sending crafted UDP messages to the targeted system. A successful exploit could allow the attacker to cause services on the device to fail, resulting in a DoS condition that could impact the targeted device and other devices that depend on it. **CVE ID : CVE-2020-3351**		190820/1141
Uncontrolled Resource Consumption	16-Jul-20	4	A vulnerability in the web-based management interface of Cisco SD-WAN vManage Software could allow an authenticated, remote attacker to consume excessive system memory and cause a denial of service (DoS) condition on an affected system. The vulnerability is due to inefficient memory management. An attacker could exploit this vulnerability by sending a large number of crafted HTTP requests to the affected web-based	N/A	H-CIS-VEDG-190820/1142

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			management interface. A successful exploit could allow the attacker to exhaust system memory, which could cause the system to stop processing new connections and could result in a DoS condition. **CVE ID : CVE-2020-3372**		
Improper Neutralization of Special Elements used in an SQL Command ('SQL Injection')	16-Jul-20	4	A vulnerability in the web-based management interface for Cisco SD-WAN vManage Software could allow an authenticated, remote attacker to impact the integrity of an affected system by executing arbitrary SQL queries. The vulnerability is due to insufficient validation of user-supplied input. An attacker could exploit this vulnerability by sending crafted input that includes SQL statements to an affected system. A successful exploit could allow the attacker to modify entries in some database tables, affecting the integrity of the data. **CVE ID : CVE-2020-3378**	N/A	H-CIS-VEDG-190820/1143
Improper Input Validation	16-Jul-20	7.2	A vulnerability in Cisco SD-WAN Solution Software could allow an authenticated, local attacker to elevate privileges to Administrator on the underlying	N/A	H-CIS-VEDG-190820/1144

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			operating system. The vulnerability is due to insufficient input validation. An attacker could exploit this vulnerability by sending a crafted request to an affected system. A successful exploit could allow the attacker to gain administrative privileges. **CVE ID : CVE-2020-3379**		
Improper Limitation of a Pathname to a Restricted Directory ('Path Traversal')	16-Jul-20	4	A vulnerability in the web-based management interface of Cisco SD-WAN vManage Software could allow an authenticated, remote attacker to conduct path traversal attacks and obtain read access to sensitive files on an affected system. The vulnerability is due to insufficient validation of HTTP requests. An attacker could exploit this vulnerability by sending a crafted HTTP request that contains directory traversal character sequences to the affected system. A successful exploit could allow the attacker to view arbitrary files on the affected system. **CVE ID : CVE-2020-3401**	N/A	H-CIS-VEDG-190820/1145
asa_5505					
Improper Input	22-Jul-20	5	A vulnerability in the web services interface of Cisco	N/A	H-CIS-ASA_-

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Validation			Adaptive Security Appliance (ASA) Software and Cisco Firepower Threat Defense (FTD) Software could allow an unauthenticated, remote attacker to conduct directory traversal attacks and read sensitive files on a targeted system. The vulnerability is due to a lack of proper input validation of URLs in HTTP requests processed by an affected device. An attacker could exploit this vulnerability by sending a crafted HTTP request containing directory traversal character sequences to an affected device. A successful exploit could allow the attacker to view arbitrary files within the web services file system on the targeted device. The web services file system is enabled when the affected device is configured with either WebVPN or AnyConnect features. This vulnerability cannot be used to obtain access to ASA or FTD system files or underlying operating system (OS) files. **CVE ID : CVE-2020-3452**		190820/1146
asa_5510					
Improper	22-Jul-20	5	A vulnerability in the web	N/A	H-CIS-ASA_-

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Input Validation			services interface of Cisco Adaptive Security Appliance (ASA) Software and Cisco Firepower Threat Defense (FTD) Software could allow an unauthenticated, remote attacker to conduct directory traversal attacks and read sensitive files on a targeted system. The vulnerability is due to a lack of proper input validation of URLs in HTTP requests processed by an affected device. An attacker could exploit this vulnerability by sending a crafted HTTP request containing directory traversal character sequences to an affected device. A successful exploit could allow the attacker to view arbitrary files within the web services file system on the targeted device. The web services file system is enabled when the affected device is configured with either WebVPN or AnyConnect features. This vulnerability cannot be used to obtain access to ASA or FTD system files or underlying operating system (OS) files. **CVE ID : CVE-2020-3452**		190820/1147
asa_5512-x					

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Improper Input Validation	22-Jul-20	5	A vulnerability in the web services interface of Cisco Adaptive Security Appliance (ASA) Software and Cisco Firepower Threat Defense (FTD) Software could allow an unauthenticated, remote attacker to conduct directory traversal attacks and read sensitive files on a targeted system. The vulnerability is due to a lack of proper input validation of URLs in HTTP requests processed by an affected device. An attacker could exploit this vulnerability by sending a crafted HTTP request containing directory traversal character sequences to an affected device. A successful exploit could allow the attacker to view arbitrary files within the web services file system on the targeted device. The web services file system is enabled when the affected device is configured with either WebVPN or AnyConnect features. This vulnerability cannot be used to obtain access to ASA or FTD system files or underlying operating system (OS) files. **CVE ID : CVE-2020-3452**	N/A	H-CIS-ASA_-190820/1148

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
asa_5515-x					
Improper Input Validation	22-Jul-20	5	A vulnerability in the web services interface of Cisco Adaptive Security Appliance (ASA) Software and Cisco Firepower Threat Defense (FTD) Software could allow an unauthenticated, remote attacker to conduct directory traversal attacks and read sensitive files on a targeted system. The vulnerability is due to a lack of proper input validation of URLs in HTTP requests processed by an affected device. An attacker could exploit this vulnerability by sending a crafted HTTP request containing directory traversal character sequences to an affected device. A successful exploit could allow the attacker to view arbitrary files within the web services file system on the targeted device. The web services file system is enabled when the affected device is configured with either WebVPN or AnyConnect features. This vulnerability cannot be used to obtain access to ASA or FTD system files or underlying operating system (OS) files.	N/A	H-CIS-ASA_-190820/1149

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2020-3452		
asa_5520					
Improper Input Validation	22-Jul-20	5	A vulnerability in the web services interface of Cisco Adaptive Security Appliance (ASA) Software and Cisco Firepower Threat Defense (FTD) Software could allow an unauthenticated, remote attacker to conduct directory traversal attacks and read sensitive files on a targeted system. The vulnerability is due to a lack of proper input validation of URLs in HTTP requests processed by an affected device. An attacker could exploit this vulnerability by sending a crafted HTTP request containing directory traversal character sequences to an affected device. A successful exploit could allow the attacker to view arbitrary files within the web services file system on the targeted device. The web services file system is enabled when the affected device is configured with either WebVPN or AnyConnect features. This vulnerability cannot be used to obtain access to ASA or FTD system files or underlying operating system (OS)	N/A	H-CIS-ASA_-190820/1150

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			files. **CVE ID : CVE-2020-3452**		
asa_5525-x					
Improper Input Validation	22-Jul-20	5	A vulnerability in the web services interface of Cisco Adaptive Security Appliance (ASA) Software and Cisco Firepower Threat Defense (FTD) Software could allow an unauthenticated, remote attacker to conduct directory traversal attacks and read sensitive files on a targeted system. The vulnerability is due to a lack of proper input validation of URLs in HTTP requests processed by an affected device. An attacker could exploit this vulnerability by sending a crafted HTTP request containing directory traversal character sequences to an affected device. A successful exploit could allow the attacker to view arbitrary files within the web services file system on the targeted device. The web services file system is enabled when the affected device is configured with either WebVPN or AnyConnect features. This vulnerability cannot be used to obtain access to ASA or FTD system files or underlying	N/A	H-CIS-ASA_-190820/1151

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			operating system (OS) files. **CVE ID : CVE-2020-3452**		
asa_5550					
Improper Input Validation	22-Jul-20	5	A vulnerability in the web services interface of Cisco Adaptive Security Appliance (ASA) Software and Cisco Firepower Threat Defense (FTD) Software could allow an unauthenticated, remote attacker to conduct directory traversal attacks and read sensitive files on a targeted system. The vulnerability is due to a lack of proper input validation of URLs in HTTP requests processed by an affected device. An attacker could exploit this vulnerability by sending a crafted HTTP request containing directory traversal character sequences to an affected device. A successful exploit could allow the attacker to view arbitrary files within the web services file system on the targeted device. The web services file system is enabled when the affected device is configured with either WebVPN or AnyConnect features. This vulnerability cannot be used to obtain access to ASA or FTD	N/A	H-CIS-ASA_-190820/1152

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			system files or underlying operating system (OS) files. **CVE ID : CVE-2020-3452**		
asa_5555-x					
Improper Input Validation	22-Jul-20	5	A vulnerability in the web services interface of Cisco Adaptive Security Appliance (ASA) Software and Cisco Firepower Threat Defense (FTD) Software could allow an unauthenticated, remote attacker to conduct directory traversal attacks and read sensitive files on a targeted system. The vulnerability is due to a lack of proper input validation of URLs in HTTP requests processed by an affected device. An attacker could exploit this vulnerability by sending a crafted HTTP request containing directory traversal character sequences to an affected device. A successful exploit could allow the attacker to view arbitrary files within the web services file system on the targeted device. The web services file system is enabled when the affected device is configured with either WebVPN or AnyConnect features. This vulnerability cannot be used to obtain	N/A	H-CIS-ASA_-190820/1153

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			access to ASA or FTD system files or underlying operating system (OS) files. **CVE ID : CVE-2020-3452**		
asa_5580					
Improper Input Validation	22-Jul-20	5	A vulnerability in the web services interface of Cisco Adaptive Security Appliance (ASA) Software and Cisco Firepower Threat Defense (FTD) Software could allow an unauthenticated, remote attacker to conduct directory traversal attacks and read sensitive files on a targeted system. The vulnerability is due to a lack of proper input validation of URLs in HTTP requests processed by an affected device. An attacker could exploit this vulnerability by sending a crafted HTTP request containing directory traversal character sequences to an affected device. A successful exploit could allow the attacker to view arbitrary files within the web services file system on the targeted device. The web services file system is enabled when the affected device is configured with either WebVPN or AnyConnect features. This vulnerability	N/A	H-CIS-ASA_-190820/1154

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			cannot be used to obtain access to ASA or FTD system files or underlying operating system (OS) files. **CVE ID : CVE-2020-3452**		
asa_5585-x					
Improper Input Validation	22-Jul-20	5	A vulnerability in the web services interface of Cisco Adaptive Security Appliance (ASA) Software and Cisco Firepower Threat Defense (FTD) Software could allow an unauthenticated, remote attacker to conduct directory traversal attacks and read sensitive files on a targeted system. The vulnerability is due to a lack of proper input validation of URLs in HTTP requests processed by an affected device. An attacker could exploit this vulnerability by sending a crafted HTTP request containing directory traversal character sequences to an affected device. A successful exploit could allow the attacker to view arbitrary files within the web services file system on the targeted device. The web services file system is enabled when the affected device is configured with either WebVPN or AnyConnect	N/A	H-CIS-ASA_-190820/1155

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			features. This vulnerability cannot be used to obtain access to ASA or FTD system files or underlying operating system (OS) files. **CVE ID : CVE-2020-3452**		
rv110w_wireless-n_vpn_firewall					
Improper Restriction of Operations within the Bounds of a Memory Buffer	16-Jul-20	9	Multiple vulnerabilities in the web-based management interface of the Cisco RV110W Wireless-N VPN Firewall, RV130 VPN Router, RV130W Wireless-N Multifunction VPN Router, and RV215W Wireless-N VPN Router could allow an authenticated, remote attacker to execute arbitrary code on an affected device. The vulnerabilities are due to improper validation of user-supplied data in the web-based management interface. An attacker could exploit these vulnerabilities by sending malicious HTTP requests to a targeted device. A successful exploit could allow the attacker to execute arbitrary code on the underlying operating system of the affected device as a high-privilege user. **CVE ID : CVE-2020-3146**	N/A	H-CIS-RV11-190820/1156

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Improper Restriction of Operations within the Bounds of a Memory Buffer	16-Jul-20	10	A vulnerability in the web-based management interface of Cisco Small Business RV110W, RV130, RV130W, and RV215W Routers could allow an unauthenticated, remote attacker to execute arbitrary code on an affected device. The vulnerability is due to improper validation of user-supplied input in the web-based management interface. An attacker could exploit this vulnerability by sending crafted HTTP requests to a targeted device. A successful exploit could allow the attacker to execute arbitrary code as the root user on the underlying operating system of the affected device. **CVE ID : CVE-2020-3323**	N/A	H-CIS-RV11-190820/1157
Use of Hard-coded Credentials	16-Jul-20	10	A vulnerability in the Telnet service of Cisco Small Business RV110W Wireless-N VPN Firewall Routers could allow an unauthenticated, remote attacker to take full control of the device with a high-privileged account. The vulnerability exists because a system account has a default and static password. An attacker could exploit this	N/A	H-CIS-RV11-190820/1158

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			vulnerability by using this default account to connect to the affected system. A successful exploit could allow the attacker to gain full control of an affected device. **CVE ID : CVE-2020-3330**		
Improper Restriction of Operations within the Bounds of a Memory Buffer	16-Jul-20	10	A vulnerability in the web-based management interface of Cisco RV110W Wireless-N VPN Firewall and Cisco RV215W Wireless-N VPN Router could allow an unauthenticated, remote attacker to execute arbitrary code on an affected device. The vulnerability is due to improper validation of user-supplied input data by the web-based management interface. An attacker could exploit this vulnerability by sending crafted requests to a targeted device. A successful exploit could allow the attacker to execute arbitrary code with the privileges of the root user. **CVE ID : CVE-2020-3331**	N/A	H-CIS-RV11-190820/1159
Improper Neutralization of Special Elements used in an OS Command	16-Jul-20	9	A vulnerability in the web-based management interface of Cisco Small Business RV110W, RV130, RV130W, and RV215W Series Routers could allow	N/A	H-CIS-RV11-190820/1160

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
('OS Command Injection')			an authenticated, remote attacker to inject arbitrary shell commands that are executed by an affected device. The vulnerability is due to insufficient input validation of user-supplied data. An attacker could exploit this vulnerability by sending a crafted request to the web-based management interface of an affected device. A successful exploit could allow the attacker to execute arbitrary shell commands or scripts with root privileges on the affected device. **CVE ID : CVE-2020-3332**		
isr1100					
Insufficiently Protected Credentials	16-Jul-20	7.2	A vulnerability in Cisco SD-WAN Solution Software could allow an unauthenticated, local attacker to access an affected device by using an account that has a default, static password. This account has root privileges. The vulnerability exists because the affected software has a user account with a default, static password. An attacker could exploit this vulnerability by remotely connecting to an affected system by using this	N/A	H-CIS-ISR1-190820/1161

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			account. A successful exploit could allow the attacker to log in by using this account with root privileges. **CVE ID : CVE-2020-3180**		
rv130_vpn_router					
Improper Restriction of Operations within the Bounds of a Memory Buffer	16-Jul-20	10	A vulnerability in the web-based management interface of Cisco Small Business RV110W, RV130, RV130W, and RV215W Routers could allow an unauthenticated, remote attacker to execute arbitrary code on an affected device. The vulnerability is due to improper validation of user-supplied input in the web-based management interface. An attacker could exploit this vulnerability by sending crafted HTTP requests to a targeted device. A successful exploit could allow the attacker to execute arbitrary code as the root user on the underlying operating system of the affected device. **CVE ID : CVE-2020-3323**	N/A	H-CIS-RV13-190820/1162
Improper Neutralization of Special Elements used in an OS Command	16-Jul-20	9	A vulnerability in the web-based management interface of Cisco Small Business RV110W, RV130, RV130W, and RV215W Series Routers could allow	N/A	H-CIS-RV13-190820/1163

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
('OS Command Injection')			an authenticated, remote attacker to inject arbitrary shell commands that are executed by an affected device. The vulnerability is due to insufficient input validation of user-supplied data. An attacker could exploit this vulnerability by sending a crafted request to the web-based management interface of an affected device. A successful exploit could allow the attacker to execute arbitrary shell commands or scripts with root privileges on the affected device. **CVE ID : CVE-2020-3332**		
rv130w_wireless-n_multifunction_vpn_router					
Improper Restriction of Operations within the Bounds of a Memory Buffer	16-Jul-20	10	A vulnerability in the web-based management interface of Cisco Small Business RV110W, RV130, RV130W, and RV215W Routers could allow an unauthenticated, remote attacker to execute arbitrary code on an affected device. The vulnerability is due to improper validation of user-supplied input in the web-based management interface. An attacker could exploit this vulnerability by sending crafted HTTP requests to a targeted device. A	N/A	H-CIS-RV13-190820/1164

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			successful exploit could allow the attacker to execute arbitrary code as the root user on the underlying operating system of the affected device. **CVE ID : CVE-2020-3323**		
Improper Neutralization of Special Elements used in an OS Command ('OS Command Injection')	16-Jul-20	9	A vulnerability in the web-based management interface of Cisco Small Business RV110W, RV130, RV130W, and RV215W Series Routers could allow an authenticated, remote attacker to inject arbitrary shell commands that are executed by an affected device. The vulnerability is due to insufficient input validation of user-supplied data. An attacker could exploit this vulnerability by sending a crafted request to the web-based management interface of an affected device. A successful exploit could allow the attacker to execute arbitrary shell commands or scripts with root privileges on the affected device. **CVE ID : CVE-2020-3332**	N/A	H-CIS-RV13-190820/1165
rv215w_wireless-n_vpn_router					
Improper Restriction of Operations within the	16-Jul-20	10	A vulnerability in the web-based management interface of Cisco Small Business RV110W, RV130, RV130W, and RV215W	N/A	H-CIS-RV21-190820/1166

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Bounds of a Memory Buffer			Routers could allow an unauthenticated, remote attacker to execute arbitrary code on an affected device. The vulnerability is due to improper validation of user-supplied input in the web-based management interface. An attacker could exploit this vulnerability by sending crafted HTTP requests to a targeted device. A successful exploit could allow the attacker to execute arbitrary code as the root user on the underlying operating system of the affected device. **CVE ID : CVE-2020-3323**		
Improper Restriction of Operations within the Bounds of a Memory Buffer	16-Jul-20	10	A vulnerability in the web-based management interface of Cisco RV110W Wireless-N VPN Firewall and Cisco RV215W Wireless-N VPN Router could allow an unauthenticated, remote attacker to execute arbitrary code on an affected device. The vulnerability is due to improper validation of user-supplied input data by the web-based management interface. An attacker could exploit this vulnerability by sending crafted requests to a	N/A	H-CIS-RV21-190820/1167

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			targeted device. A successful exploit could allow the attacker to execute arbitrary code with the privileges of the root user. **CVE ID : CVE-2020-3331**		
Improper Neutralization of Special Elements used in an OS Command ('OS Command Injection')	16-Jul-20	9	A vulnerability in the web-based management interface of Cisco Small Business RV110W, RV130, RV130W, and RV215W Series Routers could allow an authenticated, remote attacker to inject arbitrary shell commands that are executed by an affected device. The vulnerability is due to insufficient input validation of user-supplied data. An attacker could exploit this vulnerability by sending a crafted request to the web-based management interface of an affected device. A successful exploit could allow the attacker to execute arbitrary shell commands or scripts with root privileges on the affected device. **CVE ID : CVE-2020-3332**	N/A	H-CIS-RV21-190820/1168
rv340_dual_wan_gigabit_vpn_router					
Improper Input Validation	16-Jul-20	10	A vulnerability in the Secure Sockets Layer (SSL) VPN feature of Cisco Small Business RV340, RV340W, RV345, and RV345P Dual WAN Gigabit VPN Routers	N/A	H-CIS-RV34-190820/1169

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			could allow an unauthenticated, remote attacker to execute arbitrary code on an affected device or cause the device to reload, resulting in a denial of service (DoS) condition. The vulnerability exists because HTTP requests are not properly validated. An attacker could exploit this vulnerability by sending a crafted HTTP request over an SSL connection to an affected device. A successful exploit could allow the attacker to remotely execute arbitrary code on the device or cause the device to reload, resulting in a DoS condition. **CVE ID : CVE-2020-3357**		
Improper Input Validation	16-Jul-20	7.8	A vulnerability in the Secure Sockets Layer (SSL) VPN feature for Cisco Small Business RV VPN Routers could allow an unauthenticated, remote attacker to cause the device to unexpectedly restart, causing a denial of service (DoS) condition. The vulnerability is due to a lack of proper input validation of HTTP requests. An attacker could exploit this vulnerability by sending a crafted HTTP request over	N/A	H-CIS-RV34-190820/1170

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			an SSL connection to the targeted device. A successful exploit could allow the attacker to cause a reload, resulting in a DoS condition. **CVE ID : CVE-2020-3358**		
rv340w_dual_wan_gigabit_wireless-ac_vpn_router					
Improper Input Validation	16-Jul-20	10	A vulnerability in the Secure Sockets Layer (SSL) VPN feature of Cisco Small Business RV340, RV340W, RV345, and RV345P Dual WAN Gigabit VPN Routers could allow an unauthenticated, remote attacker to execute arbitrary code on an affected device or cause the device to reload, resulting in a denial of service (DoS) condition. The vulnerability exists because HTTP requests are not properly validated. An attacker could exploit this vulnerability by sending a crafted HTTP request over an SSL connection to an affected device. A successful exploit could allow the attacker to remotely execute arbitrary code on the device or cause the device to reload, resulting in a DoS condition. **CVE ID : CVE-2020-3357**	N/A	H-CIS-RV34-190820/1171
Improper Input	16-Jul-20	7.8	A vulnerability in the Secure Sockets Layer (SSL)	N/A	H-CIS-RV34-

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Validation			VPN feature for Cisco Small Business RV VPN Routers could allow an unauthenticated, remote attacker to cause the device to unexpectedly restart, causing a denial of service (DoS) condition. The vulnerability is due to a lack of proper input validation of HTTP requests. An attacker could exploit this vulnerability by sending a crafted HTTP request over an SSL connection to the targeted device. A successful exploit could allow the attacker to cause a reload, resulting in a DoS condition. **CVE ID : CVE-2020-3358**		190820/1172
rv345_dual_wan_gigabit_vpn_router					
Improper Input Validation	16-Jul-20	10	A vulnerability in the Secure Sockets Layer (SSL) VPN feature of Cisco Small Business RV340, RV340W, RV345, and RV345P Dual WAN Gigabit VPN Routers could allow an unauthenticated, remote attacker to execute arbitrary code on an affected device or cause the device to reload, resulting in a denial of service (DoS) condition. The vulnerability exists because HTTP requests are not properly validated.	N/A	H-CIS-RV34-190820/1173

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			An attacker could exploit this vulnerability by sending a crafted HTTP request over an SSL connection to an affected device. A successful exploit could allow the attacker to remotely execute arbitrary code on the device or cause the device to reload, resulting in a DoS condition. **CVE ID : CVE-2020-3357**		
Improper Input Validation	16-Jul-20	7.8	A vulnerability in the Secure Sockets Layer (SSL) VPN feature for Cisco Small Business RV VPN Routers could allow an unauthenticated, remote attacker to cause the device to unexpectedly restart, causing a denial of service (DoS) condition. The vulnerability is due to a lack of proper input validation of HTTP requests. An attacker could exploit this vulnerability by sending a crafted HTTP request over an SSL connection to the targeted device. A successful exploit could allow the attacker to cause a reload, resulting in a DoS condition. **CVE ID : CVE-2020-3358**	N/A	H-CIS-RV34-190820/1174
rv345p_dual_wan_gigabit_poe_vpn_router					
Improper Input	16-Jul-20	10	A vulnerability in the Secure Sockets Layer (SSL)	N/A	H-CIS-RV34-

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Validation			VPN feature of Cisco Small Business RV340, RV340W, RV345, and RV345P Dual WAN Gigabit VPN Routers could allow an unauthenticated, remote attacker to execute arbitrary code on an affected device or cause the device to reload, resulting in a denial of service (DoS) condition. The vulnerability exists because HTTP requests are not properly validated. An attacker could exploit this vulnerability by sending a crafted HTTP request over an SSL connection to an affected device. A successful exploit could allow the attacker to remotely execute arbitrary code on the device or cause the device to reload, resulting in a DoS condition. **CVE ID : CVE-2020-3357**		190820/1175
Improper Input Validation	16-Jul-20	7.8	A vulnerability in the Secure Sockets Layer (SSL) VPN feature for Cisco Small Business RV VPN Routers could allow an unauthenticated, remote attacker to cause the device to unexpectedly restart, causing a denial of service (DoS) condition. The vulnerability is due to a lack of proper input validation of HTTP	N/A	H-CIS-RV34-190820/1176

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			requests. An attacker could exploit this vulnerability by sending a crafted HTTP request over an SSL connection to the targeted device. A successful exploit could allow the attacker to cause a reload, resulting in a DoS condition. **CVE ID : CVE-2020-3358**		
isr1100-4gltegb					
Insufficiently Protected Credentials	16-Jul-20	7.2	A vulnerability in Cisco SD-WAN Solution Software could allow an unauthenticated, local attacker to access an affected device by using an account that has a default, static password. This account has root privileges. The vulnerability exists because the affected software has a user account with a default, static password. An attacker could exploit this vulnerability by remotely connecting to an affected system by using this account. A successful exploit could allow the attacker to log in by using this account with root privileges. **CVE ID : CVE-2020-3180**	N/A	H-CIS-ISR1-190820/1177
Uncontrolled Resource	16-Jul-20	4	A vulnerability in the web-based management interface of Cisco SD-WAN	N/A	H-CIS-ISR1-190820/1178

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Consumption			vManage Software could allow an authenticated, remote attacker to consume excessive system memory and cause a denial of service (DoS) condition on an affected system. The vulnerability is due to inefficient memory management. An attacker could exploit this vulnerability by sending a large number of crafted HTTP requests to the affected web-based management interface. A successful exploit could allow the attacker to exhaust system memory, which could cause the system to stop processing new connections and could result in a DoS condition. **CVE ID : CVE-2020-3372**		
Improper Neutralization of Special Elements used in an SQL Command ('SQL Injection')	16-Jul-20	4	A vulnerability in the web-based management interface for Cisco SD-WAN vManage Software could allow an authenticated, remote attacker to impact the integrity of an affected system by executing arbitrary SQL queries. The vulnerability is due to insufficient validation of user-supplied input. An attacker could exploit this vulnerability by sending crafted input that includes SQL statements to an	N/A	H-CIS-ISR1-190820/1179

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			affected system. A successful exploit could allow the attacker to modify entries in some database tables, affecting the integrity of the data. **CVE ID : CVE-2020-3378**		
Improper Limitation of a Pathname to a Restricted Directory ('Path Traversal')	16-Jul-20	6.5	A vulnerability in the web management interface of Cisco SD-WAN vManage Software could allow an authenticated, remote attacker to conduct directory traversal attacks and obtain read and write access to sensitive files on a targeted system. The vulnerability is due to a lack of proper validation of files that are uploaded to an affected device. An attacker could exploit this vulnerability by uploading a crafted file to an affected system. An exploit could allow the attacker to view or modify arbitrary files on the targeted system. **CVE ID : CVE-2020-3381**	N/A	H-CIS-ISR1-190820/1180
Improper Input Validation	16-Jul-20	9	A vulnerability in Cisco SD-WAN vManage Software could allow an authenticated, remote attacker to execute code with root privileges on an affected system. The vulnerability is due to insufficient input sanitization during user authentication processing.	N/A	H-CIS-ISR1-190820/1181

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			An attacker could exploit this vulnerability by sending a crafted response to the Cisco SD-WAN vManage Software. A successful exploit could allow the attacker to access the software and execute commands they should not be authorized to execute. **CVE ID : CVE-2020-3387**		
Improper Authenticati on	16-Jul-20	7.2	A vulnerability in the CLI of Cisco SD-WAN vManage Software could allow an authenticated, local attacker to inject arbitrary commands that are executed with root privileges. The vulnerability is due to insufficient input validation. An attacker could exploit this vulnerability by authenticating to the device and submitting crafted input to the CLI. The attacker must be authenticated to access the CLI. A successful exploit could allow the attacker to execute commands with root privileges. **CVE ID : CVE-2020-3388**	N/A	H-CIS-ISR1-190820/1182
Improper Limitation of a Pathname to a Restricted	16-Jul-20	4	A vulnerability in the web-based management interface of Cisco SD-WAN vManage Software could allow an authenticated,	N/A	H-CIS-ISR1-190820/1183

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Directory ('Path Traversal')			remote attacker to conduct path traversal attacks and obtain read access to sensitive files on an affected system. The vulnerability is due to insufficient validation of HTTP requests. An attacker could exploit this vulnerability by sending a crafted HTTP request that contains directory traversal character sequences to the affected system. A successful exploit could allow the attacker to view arbitrary files on the affected system. **CVE ID : CVE-2020-3401**		
isr1100-4gltena					
Insufficiently Protected Credentials	16-Jul-20	7.2	A vulnerability in Cisco SD-WAN Solution Software could allow an unauthenticated, local attacker to access an affected device by using an account that has a default, static password. This account has root privileges. The vulnerability exists because the affected software has a user account with a default, static password. An attacker could exploit this vulnerability by remotely connecting to an affected system by using this	N/A	H-CIS-ISR1-190820/1184

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			account. A successful exploit could allow the attacker to log in by using this account with root privileges. **CVE ID : CVE-2020-3180**		
Uncontrolled Resource Consumption	16-Jul-20	4	A vulnerability in the web-based management interface of Cisco SD-WAN vManage Software could allow an authenticated, remote attacker to consume excessive system memory and cause a denial of service (DoS) condition on an affected system. The vulnerability is due to inefficient memory management. An attacker could exploit this vulnerability by sending a large number of crafted HTTP requests to the affected web-based management interface. A successful exploit could allow the attacker to exhaust system memory, which could cause the system to stop processing new connections and could result in a DoS condition. **CVE ID : CVE-2020-3372**	N/A	H-CIS-ISR1-190820/1185
Improper Neutralization of Special Elements used in an SQL Command	16-Jul-20	4	A vulnerability in the web-based management interface for Cisco SD-WAN vManage Software could allow an authenticated, remote attacker to impact the	N/A	H-CIS-ISR1-190820/1186

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
('SQL Injection')			integrity of an affected system by executing arbitrary SQL queries. The vulnerability is due to insufficient validation of user-supplied input. An attacker could exploit this vulnerability by sending crafted input that includes SQL statements to an affected system. A successful exploit could allow the attacker to modify entries in some database tables, affecting the integrity of the data. **CVE ID : CVE-2020-3378**		
Improper Limitation of a Pathname to a Restricted Directory ('Path Traversal')	16-Jul-20	6.5	A vulnerability in the web management interface of Cisco SD-WAN vManage Software could allow an authenticated, remote attacker to conduct directory traversal attacks and obtain read and write access to sensitive files on a targeted system. The vulnerability is due to a lack of proper validation of files that are uploaded to an affected device. An attacker could exploit this vulnerability by uploading a crafted file to an affected system. An exploit could allow the attacker to view or modify arbitrary files on the targeted system. **CVE ID : CVE-2020-3381**	N/A	H-CIS-ISR1-190820/1187
Improper	16-Jul-20	9	A vulnerability in Cisco SD-	N/A	H-CIS-ISR1-

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Input Validation			WAN vManage Software could allow an authenticated, remote attacker to execute code with root privileges on an affected system. The vulnerability is due to insufficient input sanitization during user authentication processing. An attacker could exploit this vulnerability by sending a crafted response to the Cisco SD-WAN vManage Software. A successful exploit could allow the attacker to access the software and execute commands they should not be authorized to execute. **CVE ID : CVE-2020-3387**		190820/1188
Improper Authenticati on	16-Jul-20	7.2	A vulnerability in the CLI of Cisco SD-WAN vManage Software could allow an authenticated, local attacker to inject arbitrary commands that are executed with root privileges. The vulnerability is due to insufficient input validation. An attacker could exploit this vulnerability by authenticating to the device and submitting crafted input to the CLI. The attacker must be authenticated to access the CLI. A successful exploit	N/A	H-CIS-ISR1-190820/1189

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			could allow the attacker to execute commands with root privileges. **CVE ID : CVE-2020-3388**		
Improper Limitation of a Pathname to a Restricted Directory ('Path Traversal')	16-Jul-20	4	A vulnerability in the web-based management interface of Cisco SD-WAN vManage Software could allow an authenticated, remote attacker to conduct path traversal attacks and obtain read access to sensitive files on an affected system. The vulnerability is due to insufficient validation of HTTP requests. An attacker could exploit this vulnerability by sending a crafted HTTP request that contains directory traversal character sequences to the affected system. A successful exploit could allow the attacker to view arbitrary files on the affected system. **CVE ID : CVE-2020-3401**	N/A	H-CIS-ISR1-190820/1190
isr1100-6g					
Insufficiently Protected Credentials	16-Jul-20	7.2	A vulnerability in Cisco SD-WAN Solution Software could allow an unauthenticated, local attacker to access an affected device by using an account that has a default, static password. This account has root privileges. The	N/A	H-CIS-ISR1-190820/1191

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			vulnerability exists because the affected software has a user account with a default, static password. An attacker could exploit this vulnerability by remotely connecting to an affected system by using this account. A successful exploit could allow the attacker to log in by using this account with root privileges. **CVE ID : CVE-2020-3180**		
Uncontrolled Resource Consumption	16-Jul-20	4	A vulnerability in the web-based management interface of Cisco SD-WAN vManage Software could allow an authenticated, remote attacker to consume excessive system memory and cause a denial of service (DoS) condition on an affected system. The vulnerability is due to inefficient memory management. An attacker could exploit this vulnerability by sending a large number of crafted HTTP requests to the affected web-based management interface. A successful exploit could allow the attacker to exhaust system memory, which could cause the system to stop processing new connections and could	N/A	H-CIS-ISR1-190820/1192

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			result in a DoS condition. **CVE ID : CVE-2020-3372**		
Improper Neutralization of Special Elements used in an SQL Command ('SQL Injection')	16-Jul-20	4	A vulnerability in the web-based management interface for Cisco SD-WAN vManage Software could allow an authenticated, remote attacker to impact the integrity of an affected system by executing arbitrary SQL queries. The vulnerability is due to insufficient validation of user-supplied input. An attacker could exploit this vulnerability by sending crafted input that includes SQL statements to an affected system. A successful exploit could allow the attacker to modify entries in some database tables, affecting the integrity of the data. **CVE ID : CVE-2020-3378**	N/A	H-CIS-ISR1-190820/1193
Improper Limitation of a Pathname to a Restricted Directory ('Path Traversal')	16-Jul-20	6.5	A vulnerability in the web management interface of Cisco SD-WAN vManage Software could allow an authenticated, remote attacker to conduct directory traversal attacks and obtain read and write access to sensitive files on a targeted system. The vulnerability is due to a lack of proper validation of files that are uploaded to an affected device. An	N/A	H-CIS-ISR1-190820/1194

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			attacker could exploit this vulnerability by uploading a crafted file to an affected system. An exploit could allow the attacker to view or modify arbitrary files on the targeted system. **CVE ID : CVE-2020-3381**		
Improper Input Validation	16-Jul-20	9	A vulnerability in Cisco SD-WAN vManage Software could allow an authenticated, remote attacker to execute code with root privileges on an affected system. The vulnerability is due to insufficient input sanitization during user authentication processing. An attacker could exploit this vulnerability by sending a crafted response to the Cisco SD-WAN vManage Software. A successful exploit could allow the attacker to access the software and execute commands they should not be authorized to execute. **CVE ID : CVE-2020-3387**	N/A	H-CIS-ISR1-190820/1195
Improper Authenticati on	16-Jul-20	7.2	A vulnerability in the CLI of Cisco SD-WAN vManage Software could allow an authenticated, local attacker to inject arbitrary commands that are executed with root privileges. The vulnerability is due to	N/A	H-CIS-ISR1-190820/1196

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			insufficient input validation. An attacker could exploit this vulnerability by authenticating to the device and submitting crafted input to the CLI. The attacker must be authenticated to access the CLI. A successful exploit could allow the attacker to execute commands with root privileges. **CVE ID : CVE-2020-3388**		
Improper Limitation of a Pathname to a Restricted Directory ('Path Traversal')	16-Jul-20	4	A vulnerability in the web-based management interface of Cisco SD-WAN vManage Software could allow an authenticated, remote attacker to conduct path traversal attacks and obtain read access to sensitive files on an affected system. The vulnerability is due to insufficient validation of HTTP requests. An attacker could exploit this vulnerability by sending a crafted HTTP request that contains directory traversal character sequences to the affected system. A successful exploit could allow the attacker to view arbitrary files on the affected system. **CVE ID : CVE-2020-3401**	N/A	H-CIS-ISR1-190820/1197
vedge_100b					

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Insufficiently Protected Credentials	16-Jul-20	7.2	A vulnerability in Cisco SD-WAN Solution Software could allow an unauthenticated, local attacker to access an affected device by using an account that has a default, static password. This account has root privileges. The vulnerability exists because the affected software has a user account with a default, static password. An attacker could exploit this vulnerability by remotely connecting to an affected system by using this account. A successful exploit could allow the attacker to log in by using this account with root privileges. **CVE ID : CVE-2020-3180**	N/A	H-CIS-VEDG-190820/1198
Uncontrolled Resource Consumption	16-Jul-20	7.8	A vulnerability in Cisco SD-WAN Solution Software could allow an unauthenticated, remote attacker to cause a denial of service (DoS) condition. The vulnerability is due to improper validation of fields in Cisco SD-WAN peering messages that are encapsulated in UDP packets. An attacker could exploit this vulnerability by sending crafted UDP messages to the targeted system. A successful	N/A	H-CIS-VEDG-190820/1199

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			exploit could allow the attacker to cause services on the device to fail, resulting in a DoS condition that could impact the targeted device and other devices that depend on it. **CVE ID : CVE-2020-3351**		
Uncontrolled Resource Consumption	16-Jul-20	4	A vulnerability in the web-based management interface of Cisco SD-WAN vManage Software could allow an authenticated, remote attacker to consume excessive system memory and cause a denial of service (DoS) condition on an affected system. The vulnerability is due to inefficient memory management. An attacker could exploit this vulnerability by sending a large number of crafted HTTP requests to the affected web-based management interface. A successful exploit could allow the attacker to exhaust system memory, which could cause the system to stop processing new connections and could result in a DoS condition. **CVE ID : CVE-2020-3372**	N/A	H-CIS-VEDG-190820/1200
Improper Neutralization of Special Elements	16-Jul-20	4	A vulnerability in the web-based management interface for Cisco SD-WAN vManage Software	N/A	H-CIS-VEDG-190820/1201

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
used in an SQL Command ('SQL Injection')			could allow an authenticated, remote attacker to impact the integrity of an affected system by executing arbitrary SQL queries. The vulnerability is due to insufficient validation of user-supplied input. An attacker could exploit this vulnerability by sending crafted input that includes SQL statements to an affected system. A successful exploit could allow the attacker to modify entries in some database tables, affecting the integrity of the data. **CVE ID : CVE-2020-3378**		
Improper Input Validation	16-Jul-20	7.2	A vulnerability in Cisco SD-WAN Solution Software could allow an authenticated, local attacker to elevate privileges to Administrator on the underlying operating system. The vulnerability is due to insufficient input validation. An attacker could exploit this vulnerability by sending a crafted request to an affected system. A successful exploit could allow the attacker to gain administrative privileges. **CVE ID : CVE-2020-3379**	N/A	H-CIS-VEDG-190820/1202
Improper	16-Jul-20	4	A vulnerability in the web-	N/A	H-CIS-VEDG-

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Limitation of a Pathname to a Restricted Directory ('Path Traversal')			based management interface of Cisco SD-WAN vManage Software could allow an authenticated, remote attacker to conduct path traversal attacks and obtain read access to sensitive files on an affected system. The vulnerability is due to insufficient validation of HTTP requests. An attacker could exploit this vulnerability by sending a crafted HTTP request that contains directory traversal character sequences to the affected system. A successful exploit could allow the attacker to view arbitrary files on the affected system. **CVE ID : CVE-2020-3401**		190820/1203
Dlink					
dir-842					
Incorrect Implementation of Authentication Algorithm	23-Jul-20	5.8	This vulnerability allows network-adjacent attackers to bypass authentication on affected installations of D-Link DIR-842 3.13B05 routers. Authentication is not required to exploit this vulnerability. The specific flaw exists within the processing of HNAP GetCAPTCHAsetting requests. The issue results from the lack of proper	N/A	H-DLI-DIR--190820/1204

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			handling of sessions. An attacker can leverage this vulnerability to execute arbitrary code in the context of the device. Was ZDI-CAN-10083. **CVE ID : CVE-2020-15632**		
dap-1860					
Improper Neutralization of Special Elements used in an OS Command ('OS Command Injection')	23-Jul-20	5.8	This vulnerability allows network-adjacent attackers to execute arbitrary code on affected installations of D-Link DAP-1860 1.04B03_HOTFIX WiFi extenders. Although authentication is required to exploit this vulnerability, the existing authentication mechanism can be bypassed. The specific flaw exists within the HNAP service, which listens on TCP port 80 by default. When parsing the SOAPAction header, the process does not properly validate a user-supplied string before using it to execute a system call. An attacker can leverage this vulnerability to execute code in the context of the device. Was ZDI-CAN-10084. **CVE ID : CVE-2020-15631**	N/A	H-DLI-DAP--190820/1205
dsl-7740c					
Improper Neutralizatio	22-Jul-20	4.6	D-Link DSL-7740C does not properly validate user	N/A	H-DLI-DSL--190820/1206

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
n of Special Elements used in an OS Command ('OS Command Injection')			input, which allows an authenticated LAN user to inject arbitrary command. **CVE ID : CVE-2020-12774**		
dap-1522					
Improper Authentication	22-Jul-20	5	An authentication-bypass issue was discovered on D-Link DAP-1522 devices 1.4x before 1.10b04Beta02. There exist a few pages that are directly accessible by any unauthorized user, e.g., logout.php and login.php. This occurs because of checking the value of NO_NEED_AUTH. If the value of NO_NEED_AUTH is 1, the user has direct access to the webpage without any authentication. By appending a query string NO_NEED_AUTH with the value of 1 to any protected URL, any unauthorized user can access the application directly, as demonstrated by bsc_lan.php?NO_NEED_AUTH=1. **CVE ID : CVE-2020-15896**	N/A	H-DLI-DAP--190820/1207
D-link					
dir-867					
Authentication Bypass	23-Jul-20	5.8	This vulnerability allows network-adjacent	N/A	H-D-L-DIR--190820/1208

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Using an Alternate Path or Channel			attackers to bypass authentication on affected installations of D-Link DIR-867, DIR-878, and DIR-882 routers with firmware 1.20B10_BETA. Authentication is not required to exploit this vulnerability. The specific flaw exists within the handling of HNAP requests. The issue results from incorrect string matching logic when accessing protected pages. An attacker can leverage this vulnerability to escalate privileges and execute code in the context of the router. Was ZDI-CAN-10835. **CVE ID : CVE-2020-15633**		
dir-882					
Authentication Bypass Using an Alternate Path or Channel	23-Jul-20	5.8	This vulnerability allows network-adjacent attackers to bypass authentication on affected installations of D-Link DIR-867, DIR-878, and DIR-882 routers with firmware 1.20B10_BETA. Authentication is not required to exploit this vulnerability. The specific flaw exists within the handling of HNAP requests. The issue results from incorrect string matching logic when accessing protected pages.	N/A	H-D-L-DIR--190820/1209

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			An attacker can leverage this vulnerability to escalate privileges and execute code in the context of the router. Was ZDI-CAN-10835. **CVE ID : CVE-2020-15633**		
dap-1520					
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	22-Jul-20	7.5	An issue was discovered in apply.cgi on D-Link DAP-1520 devices before 1.10b04Beta02. Whenever a user performs a login action from the web interface, the request values are being forwarded to the ssi binary. On the login page, the web interface restricts the password input field to a fixed length of 15 characters. The problem is that validation is being done on the client side, hence it can be bypassed. When an attacker manages to intercept the login request (POST based) and tampers with the vulnerable parameter (log_pass), to a larger length, the request will be forwarded to the webserver. This results in a stack-based buffer overflow. A few other POST variables, (transferred as part of the login request) are also vulnerable:	N/A	H-D-L-DAP--190820/1210

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			html_response_page and log_user. **CVE ID : CVE-2020-15892**		
dir-816l					
Improper Neutralization of Special Elements used in an OS Command ('OS Command Injection')	22-Jul-20	7.5	An issue was discovered on D-Link DIR-816L devices 2.x before 1.10b04Beta02. Universal Plug and Play (UPnP) is enabled by default on port 1900. An attacker can perform command injection by injecting a payload into the Search Target (ST) field of the SSDP M-SEARCH discover packet. **CVE ID : CVE-2020-15893**	N/A	H-D-L-DIR--190820/1211
Information Exposure	22-Jul-20	5	An issue was discovered on D-Link DIR-816L devices 2.x before 1.10b04Beta02. There exists an exposed administration function in getcfg.php, which can be used to call various services. It can be utilized by an attacker to retrieve various sensitive information, such as admin login credentials, by setting the value of _POST_SERVICES in the query string to DEVICE.ACCOUNT. **CVE ID : CVE-2020-15894**	N/A	H-D-L-DIR--190820/1212
Improper Neutralization of Input	22-Jul-20	4.3	An XSS issue was discovered on D-Link DIR-816L devices 2.x before	N/A	H-D-L-DIR--190820/1213

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
During Web Page Generation ('Cross-site Scripting')			1.10b04Beta02. In the file webinc/js/info.php, no output filtration is applied to the RESULT parameter, before it's printed on the webpage. **CVE ID : CVE-2020-15895**		
dir-878					
Authentication Bypass Using an Alternate Path or Channel	23-Jul-20	5.8	This vulnerability allows network-adjacent attackers to bypass authentication on affected installations of D-Link DIR-867, DIR-878, and DIR-882 routers with firmware 1.20B10_BETA. Authentication is not required to exploit this vulnerability. The specific flaw exists within the handling of HNAP requests. The issue results from incorrect string matching logic when accessing protected pages. An attacker can leverage this vulnerability to escalate privileges and execute code in the context of the router. Was ZDI-CAN-10835. **CVE ID : CVE-2020-15633**	N/A	H-D-L-DIR--190820/1214
Grandstream					
gwn7000					
Improper Neutralization of Special Elements used in an OS	17-Jul-20	9	Grandstream GWN7000 firmware version 1.0.9.4 and below allows authenticated remote users to modify the	https://www.tenable.com/security/research/tra-2020-41	H-GRA-GWN7-190820/1215

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Command ('OS Command Injection')			system's crontab via undocumented API. An attacker can use this functionality to execute arbitrary OS commands on the router. **CVE ID : CVE-2020-5756**		
ucm6204					
Improper Neutralization of Special Elements used in an OS Command ('OS Command Injection')	17-Jul-20	10	Grandstream UCM6200 series firmware version 1.0.20.23 and below is vulnerable to OS command injection via SSH. An authenticated remote attacker can execute commands as the root user by issuing a specially crafted "unset" command. **CVE ID : CVE-2020-5759**	https://www.tenable.com/security/research/tra-2020-42	H-GRA-UCM6-190820/1216
Improper Neutralization of Special Elements used in an OS Command ('OS Command Injection')	17-Jul-20	10	Grandstream UCM6200 series firmware version 1.0.20.23 and below is vulnerable to OS command injection via HTTP. An authenticated remote attacker can bypass command injection mitigations and execute commands as the root user by sending a crafted HTTP POST to the UCM's "New" HTTPS API. **CVE ID : CVE-2020-5757**	https://www.tenable.com/security/research/tra-2020-42	H-GRA-UCM6-190820/1217
Improper Neutralization of Special Elements used in an OS Command	17-Jul-20	9	Grandstream UCM6200 series firmware version 1.0.20.23 and below is vulnerable to OS command injection via HTTP. An authenticated remote	https://www.tenable.com/security/research/tra-2020-42	H-GRA-UCM6-190820/1218

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
('OS Command Injection')			attacker can execute commands as the root user by sending a crafted HTTP GET to the UCM's "Old" HTTPS API. **CVE ID : CVE-2020-5758**		
ht801					
Improper Neutralization of Special Elements used in an OS Command ('OS Command Injection')	29-Jul-20	9.3	Grandstream HT800 series firmware version 1.0.17.5 and below is vulnerable to an OS command injection vulnerability. Unauthenticated remote attackers can execute arbitrary commands as root by crafting a special configuration file and sending a crafted SIP message. **CVE ID : CVE-2020-5760**	N/A	H-GRA-HT80-190820/1219
Loop with Unreachable Exit Condition ('Infinite Loop')	29-Jul-20	7.8	Grandstream HT800 series firmware version 1.0.17.5 and below is vulnerable to CPU exhaustion due to an infinite loop in the TR-069 service. Unauthenticated remote attackers can trigger this case by sending a one character TCP message to the TR-069 service. **CVE ID : CVE-2020-5761**	N/A	H-GRA-HT80-190820/1220
NULL Pointer Dereference	29-Jul-20	5	Grandstream HT800 series firmware version 1.0.17.5 and below is vulnerable to a denial of service attack against the TR-069 service. An unauthenticated remote attacker can stop	N/A	H-GRA-HT80-190820/1221

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			the service due to a NULL pointer dereference in the TR-069 service. This condition is triggered due to mishandling of the HTTP Authentication field. **CVE ID : CVE-2020-5762**		
Inadequate Encryption Strength	29-Jul-20	9	Grandstream HT800 series firmware version 1.0.17.5 and below contain a backdoor in the SSH service. An authenticated remote attacker can obtain a root shell by correctly answering a challenge prompt. **CVE ID : CVE-2020-5763**	N/A	H-GRA-HT80-190820/1222
ht802					
Improper Neutralization of Special Elements used in an OS Command ('OS Command Injection')	29-Jul-20	9.3	Grandstream HT800 series firmware version 1.0.17.5 and below is vulnerable to an OS command injection vulnerability. Unauthenticated remote attackers can execute arbitrary commands as root by crafting a special configuration file and sending a crafted SIP message. **CVE ID : CVE-2020-5760**	N/A	H-GRA-HT80-190820/1223
Loop with Unreachable Exit Condition ('Infinite Loop')	29-Jul-20	7.8	Grandstream HT800 series firmware version 1.0.17.5 and below is vulnerable to CPU exhaustion due to an infinite loop in the TR-069 service. Unauthenticated remote attackers can trigger this case by	N/A	H-GRA-HT80-190820/1224

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			sending a one character TCP message to the TR-069 service. **CVE ID : CVE-2020-5761**		
NULL Pointer Dereference	29-Jul-20	5	Grandstream HT800 series firmware version 1.0.17.5 and below is vulnerable to a denial of service attack against the TR-069 service. An unauthenticated remote attacker can stop the service due to a NULL pointer dereference in the TR-069 service. This condition is triggered due to mishandling of the HTTP Authentication field. **CVE ID : CVE-2020-5762**	N/A	H-GRA-HT80-190820/1225
Inadequate Encryption Strength	29-Jul-20	9	Grandstream HT800 series firmware version 1.0.17.5 and below contain a backdoor in the SSH service. An authenticated remote attacker can obtain a root shell by correctly answering a challenge prompt. **CVE ID : CVE-2020-5763**	N/A	H-GRA-HT80-190820/1226
ht812					
Improper Neutralization of Special Elements used in an OS Command ('OS Command Injection')	29-Jul-20	9.3	Grandstream HT800 series firmware version 1.0.17.5 and below is vulnerable to an OS command injection vulnerability. Unauthenticated remote attackers can execute arbitrary commands as root by crafting a special configuration file and	N/A	H-GRA-HT81-190820/1227

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			sending a crafted SIP message. **CVE ID : CVE-2020-5760**		
Loop with Unreachable Exit Condition ('Infinite Loop')	29-Jul-20	7.8	Grandstream HT800 series firmware version 1.0.17.5 and below is vulnerable to CPU exhaustion due to an infinite loop in the TR-069 service. Unauthenticated remote attackers can trigger this case by sending a one character TCP message to the TR-069 service. **CVE ID : CVE-2020-5761**	N/A	H-GRA-HT81-190820/1228
NULL Pointer Dereference	29-Jul-20	5	Grandstream HT800 series firmware version 1.0.17.5 and below is vulnerable to a denial of service attack against the TR-069 service. An unauthenticated remote attacker can stop the service due to a NULL pointer dereference in the TR-069 service. This condition is triggered due to mishandling of the HTTP Authentication field. **CVE ID : CVE-2020-5762**	N/A	H-GRA-HT81-190820/1229
Inadequate Encryption Strength	29-Jul-20	9	Grandstream HT800 series firmware version 1.0.17.5 and below contain a backdoor in the SSH service. An authenticated remote attacker can obtain a root shell by correctly answering a challenge prompt. **CVE ID : CVE-2020-5763**	N/A	H-GRA-HT81-190820/1230

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
ht814					
Improper Neutralization of Special Elements used in an OS Command ('OS Command Injection')	29-Jul-20	9.3	Grandstream HT800 series firmware version 1.0.17.5 and below is vulnerable to an OS command injection vulnerability. Unauthenticated remote attackers can execute arbitrary commands as root by crafting a special configuration file and sending a crafted SIP message. **CVE ID : CVE-2020-5760**	N/A	H-GRA-HT81-190820/1231
Loop with Unreachable Exit Condition ('Infinite Loop')	29-Jul-20	7.8	Grandstream HT800 series firmware version 1.0.17.5 and below is vulnerable to CPU exhaustion due to an infinite loop in the TR-069 service. Unauthenticated remote attackers can trigger this case by sending a one character TCP message to the TR-069 service. **CVE ID : CVE-2020-5761**	N/A	H-GRA-HT81-190820/1232
NULL Pointer Dereference	29-Jul-20	5	Grandstream HT800 series firmware version 1.0.17.5 and below is vulnerable to a denial of service attack against the TR-069 service. An unauthenticated remote attacker can stop the service due to a NULL pointer dereference in the TR-069 service. This condition is triggered due to mishandling of the HTTP Authentication field.	N/A	H-GRA-HT81-190820/1233

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2020-5762		
Inadequate Encryption Strength	29-Jul-20	9	Grandstream HT800 series firmware version 1.0.17.5 and below contain a backdoor in the SSH service. An authenticated remote attacker can obtain a root shell by correctly answering a challenge prompt. **CVE ID : CVE-2020-5763**	N/A	H-GRA-HT81-190820/1234
ht818					
Improper Neutralization of Special Elements used in an OS Command ('OS Command Injection')	29-Jul-20	9.3	Grandstream HT800 series firmware version 1.0.17.5 and below is vulnerable to an OS command injection vulnerability. Unauthenticated remote attackers can execute arbitrary commands as root by crafting a special configuration file and sending a crafted SIP message. **CVE ID : CVE-2020-5760**	N/A	H-GRA-HT81-190820/1235
Loop with Unreachable Exit Condition ('Infinite Loop')	29-Jul-20	7.8	Grandstream HT800 series firmware version 1.0.17.5 and below is vulnerable to CPU exhaustion due to an infinite loop in the TR-069 service. Unauthenticated remote attackers can trigger this case by sending a one character TCP message to the TR-069 service. **CVE ID : CVE-2020-5761**	N/A	H-GRA-HT81-190820/1236
NULL Pointer	29-Jul-20	5	Grandstream HT800 series firmware version 1.0.17.5	N/A	H-GRA-HT81-

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Dereference			and below is vulnerable to a denial of service attack against the TR-069 service. An unauthenticated remote attacker can stop the service due to a NULL pointer dereference in the TR-069 service. This condition is triggered due to mishandling of the HTTP Authentication field. **CVE ID : CVE-2020-5762**		190820/1237
Inadequate Encryption Strength	29-Jul-20	9	Grandstream HT800 series firmware version 1.0.17.5 and below contain a backdoor in the SSH service. An authenticated remote attacker can obtain a root shell by correctly answering a challenge prompt. **CVE ID : CVE-2020-5763**	N/A	H-GRA-HT81-190820/1238
ht813					
Improper Neutralization of Special Elements used in an OS Command ('OS Command Injection')	29-Jul-20	9.3	Grandstream HT800 series firmware version 1.0.17.5 and below is vulnerable to an OS command injection vulnerability. Unauthenticated remote attackers can execute arbitrary commands as root by crafting a special configuration file and sending a crafted SIP message. **CVE ID : CVE-2020-5760**	N/A	H-GRA-HT81-190820/1239
Loop with Unreachable Exit	29-Jul-20	7.8	Grandstream HT800 series firmware version 1.0.17.5 and below is vulnerable to	N/A	H-GRA-HT81-190820/1240

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Condition ('Infinite Loop')			CPU exhaustion due to an infinite loop in the TR-069 service. Unauthenticated remote attackers can trigger this case by sending a one character TCP message to the TR-069 service. **CVE ID : CVE-2020-5761**		
NULL Pointer Dereference	29-Jul-20	5	Grandstream HT800 series firmware version 1.0.17.5 and below is vulnerable to a denial of service attack against the TR-069 service. An unauthenticated remote attacker can stop the service due to a NULL pointer dereference in the TR-069 service. This condition is triggered due to mishandling of the HTTP Authentication field. **CVE ID : CVE-2020-5762**	N/A	H-GRA-HT81-190820/1241
Inadequate Encryption Strength	29-Jul-20	9	Grandstream HT800 series firmware version 1.0.17.5 and below contain a backdoor in the SSH service. An authenticated remote attacker can obtain a root shell by correctly answering a challenge prompt. **CVE ID : CVE-2020-5763**	N/A	H-GRA-HT81-190820/1242
ucm6202					
Improper Neutralization of Special Elements used in an OS	17-Jul-20	10	Grandstream UCM6200 series firmware version 1.0.20.23 and below is vulnerable to OS command injection via HTTP. An	https://www.tenable.com/security/research/tra-2020-42	H-GRA-UCM6-190820/1243

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Command ('OS Command Injection')			authenticated remote attacker can bypass command injection mitigations and execute commands as the root user by sending a crafted HTTP POST to the UCM's "New" HTTPS API. **CVE ID : CVE-2020-5757**		
Improper Neutralization of Special Elements used in an OS Command ('OS Command Injection')	17-Jul-20	9	Grandstream UCM6200 series firmware version 1.0.20.23 and below is vulnerable to OS command injection via HTTP. An authenticated remote attacker can execute commands as the root user by sending a crafted HTTP GET to the UCM's "Old" HTTPS API. **CVE ID : CVE-2020-5758**	https://www.tenable.com/security/research/tra-2020-42	H-GRA-UCM6-190820/1244
Improper Neutralization of Special Elements used in an OS Command ('OS Command Injection')	17-Jul-20	10	Grandstream UCM6200 series firmware version 1.0.20.23 and below is vulnerable to OS command injection via SSH. An authenticated remote attacker can execute commands as the root user by issuing a specially crafted "unset" command. **CVE ID : CVE-2020-5759**	https://www.tenable.com/security/research/tra-2020-42	H-GRA-UCM6-190820/1245
ucm6208					
Improper Neutralization of Special Elements used in an OS Command	17-Jul-20	10	Grandstream UCM6200 series firmware version 1.0.20.23 and below is vulnerable to OS command injection via SSH. An authenticated remote	https://www.tenable.com/security/research/tra-2020-42	H-GRA-UCM6-190820/1246

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
('OS Command Injection')			attacker can execute commands as the root user by issuing a specially crafted "unset" command. **CVE ID : CVE-2020-5759**		
Improper Neutralization of Special Elements used in an OS Command ('OS Command Injection')	17-Jul-20	10	Grandstream UCM6200 series firmware version 1.0.20.23 and below is vulnerable to OS command injection via HTTP. An authenticated remote attacker can bypass command injection mitigations and execute commands as the root user by sending a crafted HTTP POST to the UCM's "New" HTTPS API. **CVE ID : CVE-2020-5757**	https://www.tenable.com/security/research/tra-2020-42	H-GRA-UCM6-190820/1247
Improper Neutralization of Special Elements used in an OS Command ('OS Command Injection')	17-Jul-20	9	Grandstream UCM6200 series firmware version 1.0.20.23 and below is vulnerable to OS command injection via HTTP. An authenticated remote attacker can execute commands as the root user by sending a crafted HTTP GET to the UCM's "Old" HTTPS API. **CVE ID : CVE-2020-5758**	https://www.tenable.com/security/research/tra-2020-42	H-GRA-UCM6-190820/1248
grundfos					
cim_500					
Missing Authentication for Critical Function	17-Jul-20	5	Grundfos CIM 500 before v06.16.00 responds to unauthenticated requests for password storage files. **CVE ID : CVE-2020-10605**	https://us-cert.cisa.gov/ics/advisories/icsa-20-189-01	H-GRU-CIM_-190820/1249

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
hpe					
proliant_bl660c_gen9_server_blade					
Improper Control of Generation of Code ('Code Injection')	30-Jul-20	7.2	A potential security vulnerability has been identified in HPE Intelligent Provisioning, Service Pack for ProLiant, and HPE Scripting ToolKit. The vulnerability could be locally exploited to allow arbitrary code execution during the boot process. **Note:** This vulnerability is related to using insmod in GRUB2 in the specific impacted HPE product and HPE is addressing this issue. HPE has made the following software updates and mitigation information to resolve the vulnerability in Intelligent Provisioning, Service Pack for ProLiant, and HPE Scripting ToolKit. HPE provided latest Intelligent Provisioning, Service Pack for ProLiant, and HPE Scripting Toolkit which includes the GRUB2 patch to resolve this vulnerability. These new boot images will update GRUB2 and the Forbidden Signature Database (DBX). After the DBX is updated, users will not be able to boot to the older IP, SPP or Scripting ToolKit with Secure Boot enabled. HPE have provided a	N/A	H-HPE-PROL-190820/1250

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			standalone DBX update tool to work with Microsoft Windows, and supported Linux Operating Systems. These tools can be used to update the Forbidden Signature Database (DBX) from within the OS. **Note:** This DBX update mitigates the GRUB2 issue with insmod enabled, and the "Boot Hole" issue for HPE signed GRUB2 applications. **CVE ID : CVE-2020-7205**		
proliant_dl20_gen9_server					
Improper Control of Generation of Code ('Code Injection')	30-Jul-20	7.2	A potential security vulnerability has been identified in HPE Intelligent Provisioning, Service Pack for ProLiant, and HPE Scripting ToolKit. The vulnerability could be locally exploited to allow arbitrary code execution during the boot process. **Note:** This vulnerability is related to using insmod in GRUB2 in the specific impacted HPE product and HPE is addressing this issue. HPE has made the following software updates and mitigation information to resolve the vulnerability in Intelligent Provisioning, Service Pack for ProLiant, and HPE Scripting ToolKit.	N/A	H-HPE-PROL-190820/1251

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			HPE provided latest Intelligent Provisioning, Service Pack for ProLiant, and HPE Scripting Toolkit which includes the GRUB2 patch to resolve this vulnerability. These new boot images will update GRUB2 and the Forbidden Signature Database (DBX). After the DBX is updated, users will not be able to boot to the older IP, SPP or Scripting ToolKit with Secure Boot enabled. HPE have provided a standalone DBX update tool to work with Microsoft Windows, and supported Linux Operating Systems. These tools can be used to update the Forbidden Signature Database (DBX) from within the OS. **Note:** This DBX update mitigates the GRUB2 issue with insmod enabled, and the "Boot Hole" issue for HPE signed GRUB2 applications. **CVE ID : CVE-2020-7205**		
proliant_dl388_gen9_server					
Improper Control of Generation of Code ('Code Injection')	30-Jul-20	7.2	A potential security vulnerability has been identified in HPE Intelligent Provisioning, Service Pack for ProLiant, and HPE Scripting ToolKit. The vulnerability could be	N/A	H-HPE-PROL-190820/1252

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			locally exploited to allow arbitrary code execution during the boot process. **Note:** This vulnerability is related to using insmod in GRUB2 in the specific impacted HPE product and HPE is addressing this issue. HPE has made the following software updates and mitigation information to resolve the vulnerability in Intelligent Provisioning, Service Pack for ProLiant, and HPE Scripting ToolKit. HPE provided latest Intelligent Provisioning, Service Pack for ProLiant, and HPE Scripting Toolkit which includes the GRUB2 patch to resolve this vulnerability. These new boot images will update GRUB2 and the Forbidden Signature Database (DBX). After the DBX is updated, users will not be able to boot to the older IP, SPP or Scripting ToolKit with Secure Boot enabled. HPE have provided a standalone DBX update tool to work with Microsoft Windows, and supported Linux Operating Systems. These tools can be used to update the Forbidden Signature Database (DBX) from within the OS. **Note:**		

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			This DBX update mitigates the GRUB2 issue with insmod enabled, and the "Boot Hole" issue for HPE signed GRUB2 applications. **CVE ID : CVE-2020-7205**		
proliant_m510_server_cartridge					
Improper Control of Generation of Code ('Code Injection')	30-Jul-20	7.2	A potential security vulnerability has been identified in HPE Intelligent Provisioning, Service Pack for ProLiant, and HPE Scripting ToolKit. The vulnerability could be locally exploited to allow arbitrary code execution during the boot process. **Note:** This vulnerability is related to using insmod in GRUB2 in the specific impacted HPE product and HPE is addressing this issue. HPE has made the following software updates and mitigation information to resolve the vulnerability in Intelligent Provisioning, Service Pack for ProLiant, and HPE Scripting ToolKit. HPE provided latest Intelligent Provisioning, Service Pack for ProLiant, and HPE Scripting Toolkit which includes the GRUB2 patch to resolve this vulnerability. These new boot images will update GRUB2 and the Forbidden	N/A	H-HPE-PROL-190820/1253

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Signature Database (DBX). After the DBX is updated, users will not be able to boot to the older IP, SPP or Scripting ToolKit with Secure Boot enabled. HPE have provided a standalone DBX update tool to work with Microsoft Windows, and supported Linux Operating Systems. These tools can be used to update the Forbidden Signature Database (DBX) from within the OS. **Note:** This DBX update mitigates the GRUB2 issue with insmod enabled, and the "Boot Hole" issue for HPE signed GRUB2 applications. **CVE ID : CVE-2020-7205**		
proliant_m710x-l_server_blade					
Improper Control of Generation of Code ('Code Injection')	30-Jul-20	7.2	A potential security vulnerability has been identified in HPE Intelligent Provisioning, Service Pack for ProLiant, and HPE Scripting ToolKit. The vulnerability could be locally exploited to allow arbitrary code execution during the boot process. **Note:** This vulnerability is related to using insmod in GRUB2 in the specific impacted HPE product and HPE is addressing this issue. HPE	N/A	H-HPE-PROL-190820/1254

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			has made the following software updates and mitigation information to resolve the vulnerability in Intelligent Provisioning, Service Pack for ProLiant, and HPE Scripting ToolKit. HPE provided latest Intelligent Provisioning, Service Pack for ProLiant, and HPE Scripting Toolkit which includes the GRUB2 patch to resolve this vulnerability. These new boot images will update GRUB2 and the Forbidden Signature Database (DBX). After the DBX is updated, users will not be able to boot to the older IP, SPP or Scripting ToolKit with Secure Boot enabled. HPE have provided a standalone DBX update tool to work with Microsoft Windows, and supported Linux Operating Systems. These tools can be used to update the Forbidden Signature Database (DBX) from within the OS. **Note:** This DBX update mitigates the GRUB2 issue with insmod enabled, and the "Boot Hole" issue for HPE signed GRUB2 applications. **CVE ID : CVE-2020-7205**		
proliant_m710x_server_blade					

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Improper Control of Generation of Code ('Code Injection')	30-Jul-20	7.2	A potential security vulnerability has been identified in HPE Intelligent Provisioning, Service Pack for ProLiant, and HPE Scripting ToolKit. The vulnerability could be locally exploited to allow arbitrary code execution during the boot process. **Note:** This vulnerability is related to using insmod in GRUB2 in the specific impacted HPE product and HPE is addressing this issue. HPE has made the following software updates and mitigation information to resolve the vulnerability in Intelligent Provisioning, Service Pack for ProLiant, and HPE Scripting ToolKit. HPE provided latest Intelligent Provisioning, Service Pack for ProLiant, and HPE Scripting Toolkit which includes the GRUB2 patch to resolve this vulnerability. These new boot images will update GRUB2 and the Forbidden Signature Database (DBX). After the DBX is updated, users will not be able to boot to the older IP, SPP or Scripting ToolKit with Secure Boot enabled. HPE have provided a standalone DBX update tool to work with	N/A	H-HPE-PROL-190820/1255

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Microsoft Windows, and supported Linux Operating Systems. These tools can be used to update the Forbidden Signature Database (DBX) from within the OS. **Note:** This DBX update mitigates the GRUB2 issue with insmod enabled, and the "Boot Hole" issue for HPE signed GRUB2 applications. **CVE ID : CVE-2020-7205**		
proliant_m750_server_blade					
Improper Control of Generation of Code ('Code Injection')	30-Jul-20	7.2	A potential security vulnerability has been identified in HPE Intelligent Provisioning, Service Pack for ProLiant, and HPE Scripting ToolKit. The vulnerability could be locally exploited to allow arbitrary code execution during the boot process. **Note:** This vulnerability is related to using insmod in GRUB2 in the specific impacted HPE product and HPE is addressing this issue. HPE has made the following software updates and mitigation information to resolve the vulnerability in Intelligent Provisioning, Service Pack for ProLiant, and HPE Scripting ToolKit. HPE provided latest Intelligent Provisioning,	N/A	H-HPE-PROL-190820/1256

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Service Pack for ProLiant, and HPE Scripting Toolkit which includes the GRUB2 patch to resolve this vulnerability. These new boot images will update GRUB2 and the Forbidden Signature Database (DBX). After the DBX is updated, users will not be able to boot to the older IP, SPP or Scripting ToolKit with Secure Boot enabled. HPE have provided a standalone DBX update tool to work with Microsoft Windows, and supported Linux Operating Systems. These tools can be used to update the Forbidden Signature Database (DBX) from within the OS. **Note:** This DBX update mitigates the GRUB2 issue with insmod enabled, and the "Boot Hole" issue for HPE signed GRUB2 applications. **CVE ID : CVE-2020-7205**		
proliant_ml10_gen9_server					
Improper Control of Generation of Code ('Code Injection')	30-Jul-20	7.2	A potential security vulnerability has been identified in HPE Intelligent Provisioning, Service Pack for ProLiant, and HPE Scripting ToolKit. The vulnerability could be locally exploited to allow arbitrary code execution	N/A	H-HPE-PROL-190820/1257

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			during the boot process. **Note:** This vulnerability is related to using insmod in GRUB2 in the specific impacted HPE product and HPE is addressing this issue. HPE has made the following software updates and mitigation information to resolve the vulnerability in Intelligent Provisioning, Service Pack for ProLiant, and HPE Scripting ToolKit. HPE provided latest Intelligent Provisioning, Service Pack for ProLiant, and HPE Scripting Toolkit which includes the GRUB2 patch to resolve this vulnerability. These new boot images will update GRUB2 and the Forbidden Signature Database (DBX). After the DBX is updated, users will not be able to boot to the older IP, SPP or Scripting ToolKit with Secure Boot enabled. HPE have provided a standalone DBX update tool to work with Microsoft Windows, and supported Linux Operating Systems. These tools can be used to update the Forbidden Signature Database (DBX) from within the OS. **Note:** This DBX update mitigates the GRUB2 issue with		

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			insmod enabled, and the "Boot Hole" issue for HPE signed GRUB2 applications. **CVE ID : CVE-2020-7205**		
proliant_ml30_gen9_server					
Improper Control of Generation of Code ('Code Injection')	30-Jul-20	7.2	A potential security vulnerability has been identified in HPE Intelligent Provisioning, Service Pack for ProLiant, and HPE Scripting ToolKit. The vulnerability could be locally exploited to allow arbitrary code execution during the boot process. **Note:** This vulnerability is related to using insmod in GRUB2 in the specific impacted HPE product and HPE is addressing this issue. HPE has made the following software updates and mitigation information to resolve the vulnerability in Intelligent Provisioning, Service Pack for ProLiant, and HPE Scripting ToolKit. HPE provided latest Intelligent Provisioning, Service Pack for ProLiant, and HPE Scripting Toolkit which includes the GRUB2 patch to resolve this vulnerability. These new boot images will update GRUB2 and the Forbidden Signature Database (DBX). After the DBX is updated,	N/A	H-HPE-PROL-190820/1258

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			users will not be able to boot to the older IP, SPP or Scripting ToolKit with Secure Boot enabled. HPE have provided a standalone DBX update tool to work with Microsoft Windows, and supported Linux Operating Systems. These tools can be used to update the Forbidden Signature Database (DBX) from within the OS. **Note:** This DBX update mitigates the GRUB2 issue with insmod enabled, and the "Boot Hole" issue for HPE signed GRUB2 applications. **CVE ID : CVE-2020-7205**		
proliant_se2160w_gen9_server					
Improper Control of Generation of Code ('Code Injection')	30-Jul-20	7.2	A potential security vulnerability has been identified in HPE Intelligent Provisioning, Service Pack for ProLiant, and HPE Scripting ToolKit. The vulnerability could be locally exploited to allow arbitrary code execution during the boot process. **Note:** This vulnerability is related to using insmod in GRUB2 in the specific impacted HPE product and HPE is addressing this issue. HPE has made the following software updates and	N/A	H-HPE-PROL-190820/1259

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			mitigation information to resolve the vulnerability in Intelligent Provisioning, Service Pack for ProLiant, and HPE Scripting ToolKit. HPE provided latest Intelligent Provisioning, Service Pack for ProLiant, and HPE Scripting Toolkit which includes the GRUB2 patch to resolve this vulnerability. These new boot images will update GRUB2 and the Forbidden Signature Database (DBX). After the DBX is updated, users will not be able to boot to the older IP, SPP or Scripting ToolKit with Secure Boot enabled. HPE have provided a standalone DBX update tool to work with Microsoft Windows, and supported Linux Operating Systems. These tools can be used to update the Forbidden Signature Database (DBX) from within the OS. **Note:** This DBX update mitigates the GRUB2 issue with insmod enabled, and the "Boot Hole" issue for HPE signed GRUB2 applications. **CVE ID : CVE-2020-7205**		
proliant_xl260a_gen9_server					
Improper Control of	30-Jul-20	7.2	A potential security vulnerability has been	N/A	H-HPE-PROL-190820/1260

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Generation of Code ('Code Injection')			identified in HPE Intelligent Provisioning, Service Pack for ProLiant, and HPE Scripting ToolKit. The vulnerability could be locally exploited to allow arbitrary code execution during the boot process. **Note:** This vulnerability is related to using insmod in GRUB2 in the specific impacted HPE product and HPE is addressing this issue. HPE has made the following software updates and mitigation information to resolve the vulnerability in Intelligent Provisioning, Service Pack for ProLiant, and HPE Scripting ToolKit. HPE provided latest Intelligent Provisioning, Service Pack for ProLiant, and HPE Scripting Toolkit which includes the GRUB2 patch to resolve this vulnerability. These new boot images will update GRUB2 and the Forbidden Signature Database (DBX). After the DBX is updated, users will not be able to boot to the older IP, SPP or Scripting ToolKit with Secure Boot enabled. HPE have provided a standalone DBX update tool to work with Microsoft Windows, and supported Linux Operating		

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Systems. These tools can be used to update the Forbidden Signature Database (DBX) from within the OS. **Note:** This DBX update mitigates the GRUB2 issue with insmod enabled, and the "Boot Hole" issue for HPE signed GRUB2 applications. **CVE ID : CVE-2020-7205**		
proliant_xl270d_gen9_server					
Improper Control of Generation of Code ('Code Injection')	30-Jul-20	7.2	A potential security vulnerability has been identified in HPE Intelligent Provisioning, Service Pack for ProLiant, and HPE Scripting ToolKit. The vulnerability could be locally exploited to allow arbitrary code execution during the boot process. **Note:** This vulnerability is related to using insmod in GRUB2 in the specific impacted HPE product and HPE is addressing this issue. HPE has made the following software updates and mitigation information to resolve the vulnerability in Intelligent Provisioning, Service Pack for ProLiant, and HPE Scripting ToolKit. HPE provided latest Intelligent Provisioning, Service Pack for ProLiant, and HPE Scripting Toolkit	N/A	H-HPE-PROL-190820/1261

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			which includes the GRUB2 patch to resolve this vulnerability. These new boot images will update GRUB2 and the Forbidden Signature Database (DBX). After the DBX is updated, users will not be able to boot to the older IP, SPP or Scripting ToolKit with Secure Boot enabled. HPE have provided a standalone DBX update tool to work with Microsoft Windows, and supported Linux Operating Systems. These tools can be used to update the Forbidden Signature Database (DBX) from within the OS. **Note:** This DBX update mitigates the GRUB2 issue with insmod enabled, and the "Boot Hole" issue for HPE signed GRUB2 applications. **CVE ID : CVE-2020-7205**		
proliant_xl740f_gen9_server					
Improper Control of Generation of Code ('Code Injection')	30-Jul-20	7.2	A potential security vulnerability has been identified in HPE Intelligent Provisioning, Service Pack for ProLiant, and HPE Scripting ToolKit. The vulnerability could be locally exploited to allow arbitrary code execution during the boot process. **Note:** This	N/A	H-HPE-PROL-190820/1262

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			vulnerability is related to using insmod in GRUB2 in the specific impacted HPE product and HPE is addressing this issue. HPE has made the following software updates and mitigation information to resolve the vulnerability in Intelligent Provisioning, Service Pack for ProLiant, and HPE Scripting ToolKit. HPE provided latest Intelligent Provisioning, Service Pack for ProLiant, and HPE Scripting Toolkit which includes the GRUB2 patch to resolve this vulnerability. These new boot images will update GRUB2 and the Forbidden Signature Database (DBX). After the DBX is updated, users will not be able to boot to the older IP, SPP or Scripting ToolKit with Secure Boot enabled. HPE have provided a standalone DBX update tool to work with Microsoft Windows, and supported Linux Operating Systems. These tools can be used to update the Forbidden Signature Database (DBX) from within the OS. **Note:** This DBX update mitigates the GRUB2 issue with insmod enabled, and the "Boot Hole" issue for HPE		

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			signed GRUB2 applications. **CVE ID : CVE-2020-7205**		
proliant_xl750f_gen9_server					
Improper Control of Generation of Code ('Code Injection')	30-Jul-20	7.2	A potential security vulnerability has been identified in HPE Intelligent Provisioning, Service Pack for ProLiant, and HPE Scripting ToolKit. The vulnerability could be locally exploited to allow arbitrary code execution during the boot process. **Note:** This vulnerability is related to using insmod in GRUB2 in the specific impacted HPE product and HPE is addressing this issue. HPE has made the following software updates and mitigation information to resolve the vulnerability in Intelligent Provisioning, Service Pack for ProLiant, and HPE Scripting ToolKit. HPE provided latest Intelligent Provisioning, Service Pack for ProLiant, and HPE Scripting Toolkit which includes the GRUB2 patch to resolve this vulnerability. These new boot images will update GRUB2 and the Forbidden Signature Database (DBX). After the DBX is updated, users will not be able to boot to the older IP, SPP or	N/A	H-HPE-PROL-190820/1263

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Scripting ToolKit with Secure Boot enabled. HPE have provided a standalone DBX update tool to work with Microsoft Windows, and supported Linux Operating Systems. These tools can be used to update the Forbidden Signature Database (DBX) from within the OS. **Note:** This DBX update mitigates the GRUB2 issue with insmod enabled, and the "Boot Hole" issue for HPE signed GRUB2 applications. **CVE ID : CVE-2020-7205**		
storeeasy_1000_storage_gen9					
Improper Control of Generation of Code ('Code Injection')	30-Jul-20	7.2	A potential security vulnerability has been identified in HPE Intelligent Provisioning, Service Pack for ProLiant, and HPE Scripting ToolKit. The vulnerability could be locally exploited to allow arbitrary code execution during the boot process. **Note:** This vulnerability is related to using insmod in GRUB2 in the specific impacted HPE product and HPE is addressing this issue. HPE has made the following software updates and mitigation information to resolve the vulnerability in	N/A	H-HPE-STOR-190820/1264

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Intelligent Provisioning, Service Pack for ProLiant, and HPE Scripting ToolKit. HPE provided latest Intelligent Provisioning, Service Pack for ProLiant, and HPE Scripting Toolkit which includes the GRUB2 patch to resolve this vulnerability. These new boot images will update GRUB2 and the Forbidden Signature Database (DBX). After the DBX is updated, users will not be able to boot to the older IP, SPP or Scripting ToolKit with Secure Boot enabled. HPE have provided a standalone DBX update tool to work with Microsoft Windows, and supported Linux Operating Systems. These tools can be used to update the Forbidden Signature Database (DBX) from within the OS. **Note:** This DBX update mitigates the GRUB2 issue with insmod enabled, and the "Boot Hole" issue for HPE signed GRUB2 applications. **CVE ID : CVE-2020-7205**		
synergy_660_gen9_compute_module					
Improper Control of Generation of Code	30-Jul-20	7.2	A potential security vulnerability has been identified in HPE Intelligent Provisioning,	N/A	H-HPE-SYNE-190820/1265

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
('Code Injection')			Service Pack for ProLiant, and HPE Scripting ToolKit. The vulnerability could be locally exploited to allow arbitrary code execution during the boot process. **Note:** This vulnerability is related to using insmod in GRUB2 in the specific impacted HPE product and HPE is addressing this issue. HPE has made the following software updates and mitigation information to resolve the vulnerability in Intelligent Provisioning, Service Pack for ProLiant, and HPE Scripting ToolKit. HPE provided latest Intelligent Provisioning, Service Pack for ProLiant, and HPE Scripting Toolkit which includes the GRUB2 patch to resolve this vulnerability. These new boot images will update GRUB2 and the Forbidden Signature Database (DBX). After the DBX is updated, users will not be able to boot to the older IP, SPP or Scripting ToolKit with Secure Boot enabled. HPE have provided a standalone DBX update tool to work with Microsoft Windows, and supported Linux Operating Systems. These tools can be used to update the		

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Forbidden Signature Database (DBX) from within the OS. **Note:** This DBX update mitigates the GRUB2 issue with insmod enabled, and the "Boot Hole" issue for HPE signed GRUB2 applications. **CVE ID : CVE-2020-7205**		
synergy_d3940_storage_module					
Improper Control of Generation of Code ('Code Injection')	30-Jul-20	7.2	A potential security vulnerability has been identified in HPE Intelligent Provisioning, Service Pack for ProLiant, and HPE Scripting ToolKit. The vulnerability could be locally exploited to allow arbitrary code execution during the boot process. **Note:** This vulnerability is related to using insmod in GRUB2 in the specific impacted HPE product and HPE is addressing this issue. HPE has made the following software updates and mitigation information to resolve the vulnerability in Intelligent Provisioning, Service Pack for ProLiant, and HPE Scripting ToolKit. HPE provided latest Intelligent Provisioning, Service Pack for ProLiant, and HPE Scripting Toolkit which includes the GRUB2 patch to resolve this	N/A	H-HPE-SYNE-190820/1266

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			vulnerability. These new boot images will update GRUB2 and the Forbidden Signature Database (DBX). After the DBX is updated, users will not be able to boot to the older IP, SPP or Scripting ToolKit with Secure Boot enabled. HPE have provided a standalone DBX update tool to work with Microsoft Windows, and supported Linux Operating Systems. These tools can be used to update the Forbidden Signature Database (DBX) from within the OS. **Note:** This DBX update mitigates the GRUB2 issue with insmod enabled, and the "Boot Hole" issue for HPE signed GRUB2 applications. **CVE ID : CVE-2020-7205**		
apollo_2000_gen10_plus_system					
Improper Control of Generation of Code ('Code Injection')	30-Jul-20	7.2	A potential security vulnerability has been identified in HPE Intelligent Provisioning, Service Pack for ProLiant, and HPE Scripting ToolKit. The vulnerability could be locally exploited to allow arbitrary code execution during the boot process. **Note:** This vulnerability is related to using insmod in GRUB2 in	N/A	H-HPE-APOL-190820/1267

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			the specific impacted HPE product and HPE is addressing this issue. HPE has made the following software updates and mitigation information to resolve the vulnerability in Intelligent Provisioning, Service Pack for ProLiant, and HPE Scripting ToolKit. HPE provided latest Intelligent Provisioning, Service Pack for ProLiant, and HPE Scripting Toolkit which includes the GRUB2 patch to resolve this vulnerability. These new boot images will update GRUB2 and the Forbidden Signature Database (DBX). After the DBX is updated, users will not be able to boot to the older IP, SPP or Scripting ToolKit with Secure Boot enabled. HPE have provided a standalone DBX update tool to work with Microsoft Windows, and supported Linux Operating Systems. These tools can be used to update the Forbidden Signature Database (DBX) from within the OS. **Note:** This DBX update mitigates the GRUB2 issue with insmod enabled, and the "Boot Hole" issue for HPE signed GRUB2 applications.		

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2020-7205		
apollo_4510_gen10_system					
Improper Control of Generation of Code ('Code Injection')	30-Jul-20	7.2	A potential security vulnerability has been identified in HPE Intelligent Provisioning, Service Pack for ProLiant, and HPE Scripting ToolKit. The vulnerability could be locally exploited to allow arbitrary code execution during the boot process. **Note:** This vulnerability is related to using insmod in GRUB2 in the specific impacted HPE product and HPE is addressing this issue. HPE has made the following software updates and mitigation information to resolve the vulnerability in Intelligent Provisioning, Service Pack for ProLiant, and HPE Scripting ToolKit. HPE provided latest Intelligent Provisioning, Service Pack for ProLiant, and HPE Scripting Toolkit which includes the GRUB2 patch to resolve this vulnerability. These new boot images will update GRUB2 and the Forbidden Signature Database (DBX). After the DBX is updated, users will not be able to boot to the older IP, SPP or Scripting ToolKit with Secure Boot enabled. HPE have provided a	N/A	H-HPE-APOL-190820/1268

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			standalone DBX update tool to work with Microsoft Windows, and supported Linux Operating Systems. These tools can be used to update the Forbidden Signature Database (DBX) from within the OS. **Note:** This DBX update mitigates the GRUB2 issue with insmod enabled, and the "Boot Hole" issue for HPE signed GRUB2 applications. **CVE ID : CVE-2020-7205**		
apollo_6500_gen10_system					
Improper Control of Generation of Code ('Code Injection')	30-Jul-20	7.2	A potential security vulnerability has been identified in HPE Intelligent Provisioning, Service Pack for ProLiant, and HPE Scripting ToolKit. The vulnerability could be locally exploited to allow arbitrary code execution during the boot process. **Note:** This vulnerability is related to using insmod in GRUB2 in the specific impacted HPE product and HPE is addressing this issue. HPE has made the following software updates and mitigation information to resolve the vulnerability in Intelligent Provisioning, Service Pack for ProLiant, and HPE Scripting ToolKit.	N/A	H-HPE-APOL-190820/1269

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			HPE provided latest Intelligent Provisioning, Service Pack for ProLiant, and HPE Scripting Toolkit which includes the GRUB2 patch to resolve this vulnerability. These new boot images will update GRUB2 and the Forbidden Signature Database (DBX). After the DBX is updated, users will not be able to boot to the older IP, SPP or Scripting ToolKit with Secure Boot enabled. HPE have provided a standalone DBX update tool to work with Microsoft Windows, and supported Linux Operating Systems. These tools can be used to update the Forbidden Signature Database (DBX) from within the OS. **Note:** This DBX update mitigates the GRUB2 issue with insmod enabled, and the "Boot Hole" issue for HPE signed GRUB2 applications. **CVE ID : CVE-2020-7205**		
cloudline_cl2100_gen10_server					
Improper Control of Generation of Code ('Code Injection')	30-Jul-20	7.2	A potential security vulnerability has been identified in HPE Intelligent Provisioning, Service Pack for ProLiant, and HPE Scripting ToolKit. The vulnerability could be	N/A	H-HPE-CLOU-190820/1270

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			locally exploited to allow arbitrary code execution during the boot process. **Note:** This vulnerability is related to using insmod in GRUB2 in the specific impacted HPE product and HPE is addressing this issue. HPE has made the following software updates and mitigation information to resolve the vulnerability in Intelligent Provisioning, Service Pack for ProLiant, and HPE Scripting ToolKit. HPE provided latest Intelligent Provisioning, Service Pack for ProLiant, and HPE Scripting Toolkit which includes the GRUB2 patch to resolve this vulnerability. These new boot images will update GRUB2 and the Forbidden Signature Database (DBX). After the DBX is updated, users will not be able to boot to the older IP, SPP or Scripting ToolKit with Secure Boot enabled. HPE have provided a standalone DBX update tool to work with Microsoft Windows, and supported Linux Operating Systems. These tools can be used to update the Forbidden Signature Database (DBX) from within the OS. **Note:**		

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			This DBX update mitigates the GRUB2 issue with insmod enabled, and the "Boot Hole" issue for HPE signed GRUB2 applications. **CVE ID : CVE-2020-7205**		
cloudline_cl2200_gen10_server					
Improper Control of Generation of Code ('Code Injection')	30-Jul-20	7.2	A potential security vulnerability has been identified in HPE Intelligent Provisioning, Service Pack for ProLiant, and HPE Scripting ToolKit. The vulnerability could be locally exploited to allow arbitrary code execution during the boot process. **Note:** This vulnerability is related to using insmod in GRUB2 in the specific impacted HPE product and HPE is addressing this issue. HPE has made the following software updates and mitigation information to resolve the vulnerability in Intelligent Provisioning, Service Pack for ProLiant, and HPE Scripting ToolKit. HPE provided latest Intelligent Provisioning, Service Pack for ProLiant, and HPE Scripting Toolkit which includes the GRUB2 patch to resolve this vulnerability. These new boot images will update GRUB2 and the Forbidden	N/A	H-HPE-CLOU-190820/1271

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Signature Database (DBX). After the DBX is updated, users will not be able to boot to the older IP, SPP or Scripting ToolKit with Secure Boot enabled. HPE have provided a standalone DBX update tool to work with Microsoft Windows, and supported Linux Operating Systems. These tools can be used to update the Forbidden Signature Database (DBX) from within the OS. **Note:** This DBX update mitigates the GRUB2 issue with insmod enabled, and the "Boot Hole" issue for HPE signed GRUB2 applications. **CVE ID : CVE-2020-7205**		
cloudline_cl2600_gen10_server					
Improper Control of Generation of Code ('Code Injection')	30-Jul-20	7.2	A potential security vulnerability has been identified in HPE Intelligent Provisioning, Service Pack for ProLiant, and HPE Scripting ToolKit. The vulnerability could be locally exploited to allow arbitrary code execution during the boot process. **Note:** This vulnerability is related to using insmod in GRUB2 in the specific impacted HPE product and HPE is addressing this issue. HPE	N/A	H-HPE-CLOU-190820/1272

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			has made the following software updates and mitigation information to resolve the vulnerability in Intelligent Provisioning, Service Pack for ProLiant, and HPE Scripting ToolKit. HPE provided latest Intelligent Provisioning, Service Pack for ProLiant, and HPE Scripting Toolkit which includes the GRUB2 patch to resolve this vulnerability. These new boot images will update GRUB2 and the Forbidden Signature Database (DBX). After the DBX is updated, users will not be able to boot to the older IP, SPP or Scripting ToolKit with Secure Boot enabled. HPE have provided a standalone DBX update tool to work with Microsoft Windows, and supported Linux Operating Systems. These tools can be used to update the Forbidden Signature Database (DBX) from within the OS. **Note:** This DBX update mitigates the GRUB2 issue with insmod enabled, and the "Boot Hole" issue for HPE signed GRUB2 applications. **CVE ID : CVE-2020-7205**		
cloudline_cl2800_gen10_server					

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Improper Control of Generation of Code ('Code Injection')	30-Jul-20	7.2	A potential security vulnerability has been identified in HPE Intelligent Provisioning, Service Pack for ProLiant, and HPE Scripting ToolKit. The vulnerability could be locally exploited to allow arbitrary code execution during the boot process. **Note:** This vulnerability is related to using insmod in GRUB2 in the specific impacted HPE product and HPE is addressing this issue. HPE has made the following software updates and mitigation information to resolve the vulnerability in Intelligent Provisioning, Service Pack for ProLiant, and HPE Scripting ToolKit. HPE provided latest Intelligent Provisioning, Service Pack for ProLiant, and HPE Scripting Toolkit which includes the GRUB2 patch to resolve this vulnerability. These new boot images will update GRUB2 and the Forbidden Signature Database (DBX). After the DBX is updated, users will not be able to boot to the older IP, SPP or Scripting ToolKit with Secure Boot enabled. HPE have provided a standalone DBX update tool to work with	N/A	H-HPE-CLOU-190820/1273

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Microsoft Windows, and supported Linux Operating Systems. These tools can be used to update the Forbidden Signature Database (DBX) from within the OS. **Note:** This DBX update mitigates the GRUB2 issue with insmod enabled, and the "Boot Hole" issue for HPE signed GRUB2 applications. **CVE ID : CVE-2020-7205**		
cloudline_cl3100_gen10_server					
Improper Control of Generation of Code ('Code Injection')	30-Jul-20	7.2	A potential security vulnerability has been identified in HPE Intelligent Provisioning, Service Pack for ProLiant, and HPE Scripting ToolKit. The vulnerability could be locally exploited to allow arbitrary code execution during the boot process. **Note:** This vulnerability is related to using insmod in GRUB2 in the specific impacted HPE product and HPE is addressing this issue. HPE has made the following software updates and mitigation information to resolve the vulnerability in Intelligent Provisioning, Service Pack for ProLiant, and HPE Scripting ToolKit. HPE provided latest Intelligent Provisioning,	N/A	H-HPE-CLOU-190820/1274

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Service Pack for ProLiant, and HPE Scripting Toolkit which includes the GRUB2 patch to resolve this vulnerability. These new boot images will update GRUB2 and the Forbidden Signature Database (DBX). After the DBX is updated, users will not be able to boot to the older IP, SPP or Scripting ToolKit with Secure Boot enabled. HPE have provided a standalone DBX update tool to work with Microsoft Windows, and supported Linux Operating Systems. These tools can be used to update the Forbidden Signature Database (DBX) from within the OS. **Note:** This DBX update mitigates the GRUB2 issue with insmod enabled, and the "Boot Hole" issue for HPE signed GRUB2 applications. **CVE ID : CVE-2020-7205**		
cloudline_cl3150_gen10_server					
Improper Control of Generation of Code ('Code Injection')	30-Jul-20	7.2	A potential security vulnerability has been identified in HPE Intelligent Provisioning, Service Pack for ProLiant, and HPE Scripting ToolKit. The vulnerability could be locally exploited to allow arbitrary code execution	N/A	H-HPE-CLOU-190820/1275

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			during the boot process. **Note:** This vulnerability is related to using insmod in GRUB2 in the specific impacted HPE product and HPE is addressing this issue. HPE has made the following software updates and mitigation information to resolve the vulnerability in Intelligent Provisioning, Service Pack for ProLiant, and HPE Scripting ToolKit. HPE provided latest Intelligent Provisioning, Service Pack for ProLiant, and HPE Scripting Toolkit which includes the GRUB2 patch to resolve this vulnerability. These new boot images will update GRUB2 and the Forbidden Signature Database (DBX). After the DBX is updated, users will not be able to boot to the older IP, SPP or Scripting ToolKit with Secure Boot enabled. HPE have provided a standalone DBX update tool to work with Microsoft Windows, and supported Linux Operating Systems. These tools can be used to update the Forbidden Signature Database (DBX) from within the OS. **Note:** This DBX update mitigates the GRUB2 issue with		

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			insmod enabled, and the "Boot Hole" issue for HPE signed GRUB2 applications. **CVE ID : CVE-2020-7205**		
cloudline_cl4100_gen10_server					
Improper Control of Generation of Code ('Code Injection')	30-Jul-20	7.2	A potential security vulnerability has been identified in HPE Intelligent Provisioning, Service Pack for ProLiant, and HPE Scripting ToolKit. The vulnerability could be locally exploited to allow arbitrary code execution during the boot process. **Note:** This vulnerability is related to using insmod in GRUB2 in the specific impacted HPE product and HPE is addressing this issue. HPE has made the following software updates and mitigation information to resolve the vulnerability in Intelligent Provisioning, Service Pack for ProLiant, and HPE Scripting ToolKit. HPE provided latest Intelligent Provisioning, Service Pack for ProLiant, and HPE Scripting Toolkit which includes the GRUB2 patch to resolve this vulnerability. These new boot images will update GRUB2 and the Forbidden Signature Database (DBX). After the DBX is updated,	N/A	H-HPE-CLOU-190820/1276

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			users will not be able to boot to the older IP, SPP or Scripting ToolKit with Secure Boot enabled. HPE have provided a standalone DBX update tool to work with Microsoft Windows, and supported Linux Operating Systems. These tools can be used to update the Forbidden Signature Database (DBX) from within the OS. **Note:** This DBX update mitigates the GRUB2 issue with insmod enabled, and the "Boot Hole" issue for HPE signed GRUB2 applications. **CVE ID : CVE-2020-7205**		
proliant_dl20_gen10_server					
Improper Control of Generation of Code ('Code Injection')	30-Jul-20	7.2	A potential security vulnerability has been identified in HPE Intelligent Provisioning, Service Pack for ProLiant, and HPE Scripting ToolKit. The vulnerability could be locally exploited to allow arbitrary code execution during the boot process. **Note:** This vulnerability is related to using insmod in GRUB2 in the specific impacted HPE product and HPE is addressing this issue. HPE has made the following software updates and	N/A	H-HPE-PROL-190820/1277

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			mitigation information to resolve the vulnerability in Intelligent Provisioning, Service Pack for ProLiant, and HPE Scripting ToolKit. HPE provided latest Intelligent Provisioning, Service Pack for ProLiant, and HPE Scripting Toolkit which includes the GRUB2 patch to resolve this vulnerability. These new boot images will update GRUB2 and the Forbidden Signature Database (DBX). After the DBX is updated, users will not be able to boot to the older IP, SPP or Scripting ToolKit with Secure Boot enabled. HPE have provided a standalone DBX update tool to work with Microsoft Windows, and supported Linux Operating Systems. These tools can be used to update the Forbidden Signature Database (DBX) from within the OS. **Note:** This DBX update mitigates the GRUB2 issue with insmod enabled, and the "Boot Hole" issue for HPE signed GRUB2 applications. **CVE ID : CVE-2020-7205**		
proliant_dl325_gen10_server					
Improper Control of	30-Jul-20	7.2	A potential security vulnerability has been	N/A	H-HPE-PROL-190820/1278

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Generation of Code ('Code Injection')			identified in HPE Intelligent Provisioning, Service Pack for ProLiant, and HPE Scripting ToolKit. The vulnerability could be locally exploited to allow arbitrary code execution during the boot process. **Note:** This vulnerability is related to using insmod in GRUB2 in the specific impacted HPE product and HPE is addressing this issue. HPE has made the following software updates and mitigation information to resolve the vulnerability in Intelligent Provisioning, Service Pack for ProLiant, and HPE Scripting ToolKit. HPE provided latest Intelligent Provisioning, Service Pack for ProLiant, and HPE Scripting Toolkit which includes the GRUB2 patch to resolve this vulnerability. These new boot images will update GRUB2 and the Forbidden Signature Database (DBX). After the DBX is updated, users will not be able to boot to the older IP, SPP or Scripting ToolKit with Secure Boot enabled. HPE have provided a standalone DBX update tool to work with Microsoft Windows, and supported Linux Operating		

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Systems. These tools can be used to update the Forbidden Signature Database (DBX) from within the OS. **Note:** This DBX update mitigates the GRUB2 issue with insmod enabled, and the "Boot Hole" issue for HPE signed GRUB2 applications. **CVE ID : CVE-2020-7205**		
proliant_dl385_gen10_server					
Improper Control of Generation of Code ('Code Injection')	30-Jul-20	7.2	A potential security vulnerability has been identified in HPE Intelligent Provisioning, Service Pack for ProLiant, and HPE Scripting ToolKit. The vulnerability could be locally exploited to allow arbitrary code execution during the boot process. **Note:** This vulnerability is related to using insmod in GRUB2 in the specific impacted HPE product and HPE is addressing this issue. HPE has made the following software updates and mitigation information to resolve the vulnerability in Intelligent Provisioning, Service Pack for ProLiant, and HPE Scripting ToolKit. HPE provided latest Intelligent Provisioning, Service Pack for ProLiant, and HPE Scripting Toolkit	N/A	H-HPE-PROL-190820/1279

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			which includes the GRUB2 patch to resolve this vulnerability. These new boot images will update GRUB2 and the Forbidden Signature Database (DBX). After the DBX is updated, users will not be able to boot to the older IP, SPP or Scripting ToolKit with Secure Boot enabled. HPE have provided a standalone DBX update tool to work with Microsoft Windows, and supported Linux Operating Systems. These tools can be used to update the Forbidden Signature Database (DBX) from within the OS. **Note:** This DBX update mitigates the GRUB2 issue with insmod enabled, and the "Boot Hole" issue for HPE signed GRUB2 applications. **CVE ID : CVE-2020-7205**		
proliant_dx170r_gen10_server					
Improper Control of Generation of Code ('Code Injection')	30-Jul-20	7.2	A potential security vulnerability has been identified in HPE Intelligent Provisioning, Service Pack for ProLiant, and HPE Scripting ToolKit. The vulnerability could be locally exploited to allow arbitrary code execution during the boot process. **Note:** This	N/A	H-HPE-PROL-190820/1280

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			vulnerability is related to using insmod in GRUB2 in the specific impacted HPE product and HPE is addressing this issue. HPE has made the following software updates and mitigation information to resolve the vulnerability in Intelligent Provisioning, Service Pack for ProLiant, and HPE Scripting ToolKit. HPE provided latest Intelligent Provisioning, Service Pack for ProLiant, and HPE Scripting Toolkit which includes the GRUB2 patch to resolve this vulnerability. These new boot images will update GRUB2 and the Forbidden Signature Database (DBX). After the DBX is updated, users will not be able to boot to the older IP, SPP or Scripting ToolKit with Secure Boot enabled. HPE have provided a standalone DBX update tool to work with Microsoft Windows, and supported Linux Operating Systems. These tools can be used to update the Forbidden Signature Database (DBX) from within the OS. **Note:** This DBX update mitigates the GRUB2 issue with insmod enabled, and the "Boot Hole" issue for HPE		

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			signed GRUB2 applications. **CVE ID : CVE-2020-7205**		
proliant_dx190r_gen10_server					
Improper Control of Generation of Code ('Code Injection')	30-Jul-20	7.2	A potential security vulnerability has been identified in HPE Intelligent Provisioning, Service Pack for ProLiant, and HPE Scripting ToolKit. The vulnerability could be locally exploited to allow arbitrary code execution during the boot process. **Note:** This vulnerability is related to using insmod in GRUB2 in the specific impacted HPE product and HPE is addressing this issue. HPE has made the following software updates and mitigation information to resolve the vulnerability in Intelligent Provisioning, Service Pack for ProLiant, and HPE Scripting ToolKit. HPE provided latest Intelligent Provisioning, Service Pack for ProLiant, and HPE Scripting Toolkit which includes the GRUB2 patch to resolve this vulnerability. These new boot images will update GRUB2 and the Forbidden Signature Database (DBX). After the DBX is updated, users will not be able to boot to the older IP, SPP or	N/A	H-HPE-PROL-190820/1281

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Scripting ToolKit with Secure Boot enabled. HPE have provided a standalone DBX update tool to work with Microsoft Windows, and supported Linux Operating Systems. These tools can be used to update the Forbidden Signature Database (DBX) from within the OS. **Note:** This DBX update mitigates the GRUB2 issue with insmod enabled, and the "Boot Hole" issue for HPE signed GRUB2 applications. **CVE ID : CVE-2020-7205**		
proliant_dx360_gen10_server					
Improper Control of Generation of Code ('Code Injection')	30-Jul-20	7.2	A potential security vulnerability has been identified in HPE Intelligent Provisioning, Service Pack for ProLiant, and HPE Scripting ToolKit. The vulnerability could be locally exploited to allow arbitrary code execution during the boot process. **Note:** This vulnerability is related to using insmod in GRUB2 in the specific impacted HPE product and HPE is addressing this issue. HPE has made the following software updates and mitigation information to resolve the vulnerability in	N/A	H-HPE-PROL-190820/1282

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Intelligent Provisioning, Service Pack for ProLiant, and HPE Scripting ToolKit. HPE provided latest Intelligent Provisioning, Service Pack for ProLiant, and HPE Scripting Toolkit which includes the GRUB2 patch to resolve this vulnerability. These new boot images will update GRUB2 and the Forbidden Signature Database (DBX). After the DBX is updated, users will not be able to boot to the older IP, SPP or Scripting ToolKit with Secure Boot enabled. HPE have provided a standalone DBX update tool to work with Microsoft Windows, and supported Linux Operating Systems. These tools can be used to update the Forbidden Signature Database (DBX) from within the OS. **Note:** This DBX update mitigates the GRUB2 issue with insmod enabled, and the "Boot Hole" issue for HPE signed GRUB2 applications. **CVE ID : CVE-2020-7205**		
proliant_dx380_gen10_server					
Improper Control of Generation of Code	30-Jul-20	7.2	A potential security vulnerability has been identified in HPE Intelligent Provisioning,	N/A	H-HPE-PROL-190820/1283

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
('Code Injection')			Service Pack for ProLiant, and HPE Scripting ToolKit. The vulnerability could be locally exploited to allow arbitrary code execution during the boot process. **Note:** This vulnerability is related to using insmod in GRUB2 in the specific impacted HPE product and HPE is addressing this issue. HPE has made the following software updates and mitigation information to resolve the vulnerability in Intelligent Provisioning, Service Pack for ProLiant, and HPE Scripting ToolKit. HPE provided latest Intelligent Provisioning, Service Pack for ProLiant, and HPE Scripting Toolkit which includes the GRUB2 patch to resolve this vulnerability. These new boot images will update GRUB2 and the Forbidden Signature Database (DBX). After the DBX is updated, users will not be able to boot to the older IP, SPP or Scripting ToolKit with Secure Boot enabled. HPE have provided a standalone DBX update tool to work with Microsoft Windows, and supported Linux Operating Systems. These tools can be used to update the		

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Forbidden Signature Database (DBX) from within the OS. **Note:** This DBX update mitigates the GRUB2 issue with insmod enabled, and the "Boot Hole" issue for HPE signed GRUB2 applications. **CVE ID : CVE-2020-7205**		
proliant_dx385_gen10_plus_server					
Improper Control of Generation of Code ('Code Injection')	30-Jul-20	7.2	A potential security vulnerability has been identified in HPE Intelligent Provisioning, Service Pack for ProLiant, and HPE Scripting ToolKit. The vulnerability could be locally exploited to allow arbitrary code execution during the boot process. **Note:** This vulnerability is related to using insmod in GRUB2 in the specific impacted HPE product and HPE is addressing this issue. HPE has made the following software updates and mitigation information to resolve the vulnerability in Intelligent Provisioning, Service Pack for ProLiant, and HPE Scripting ToolKit. HPE provided latest Intelligent Provisioning, Service Pack for ProLiant, and HPE Scripting Toolkit which includes the GRUB2 patch to resolve this	N/A	H-HPE-PROL-190820/1284

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			vulnerability. These new boot images will update GRUB2 and the Forbidden Signature Database (DBX). After the DBX is updated, users will not be able to boot to the older IP, SPP or Scripting ToolKit with Secure Boot enabled. HPE have provided a standalone DBX update tool to work with Microsoft Windows, and supported Linux Operating Systems. These tools can be used to update the Forbidden Signature Database (DBX) from within the OS. **Note:** This DBX update mitigates the GRUB2 issue with insmod enabled, and the "Boot Hole" issue for HPE signed GRUB2 applications. **CVE ID : CVE-2020-7205**		
proliant_dx4200_gen10_server					
Improper Control of Generation of Code ('Code Injection')	30-Jul-20	7.2	A potential security vulnerability has been identified in HPE Intelligent Provisioning, Service Pack for ProLiant, and HPE Scripting ToolKit. The vulnerability could be locally exploited to allow arbitrary code execution during the boot process. **Note:** This vulnerability is related to using insmod in GRUB2 in	N/A	H-HPE-PROL-190820/1285

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			the specific impacted HPE product and HPE is addressing this issue. HPE has made the following software updates and mitigation information to resolve the vulnerability in Intelligent Provisioning, Service Pack for ProLiant, and HPE Scripting ToolKit. HPE provided latest Intelligent Provisioning, Service Pack for ProLiant, and HPE Scripting Toolkit which includes the GRUB2 patch to resolve this vulnerability. These new boot images will update GRUB2 and the Forbidden Signature Database (DBX). After the DBX is updated, users will not be able to boot to the older IP, SPP or Scripting ToolKit with Secure Boot enabled. HPE have provided a standalone DBX update tool to work with Microsoft Windows, and supported Linux Operating Systems. These tools can be used to update the Forbidden Signature Database (DBX) from within the OS. **Note:** This DBX update mitigates the GRUB2 issue with insmod enabled, and the "Boot Hole" issue for HPE signed GRUB2 applications.		

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2020-7205		
proliant_dx560_gen10_server					
Improper Control of Generation of Code ('Code Injection')	30-Jul-20	7.2	A potential security vulnerability has been identified in HPE Intelligent Provisioning, Service Pack for ProLiant, and HPE Scripting ToolKit. The vulnerability could be locally exploited to allow arbitrary code execution during the boot process. **Note:** This vulnerability is related to using insmod in GRUB2 in the specific impacted HPE product and HPE is addressing this issue. HPE has made the following software updates and mitigation information to resolve the vulnerability in Intelligent Provisioning, Service Pack for ProLiant, and HPE Scripting ToolKit. HPE provided latest Intelligent Provisioning, Service Pack for ProLiant, and HPE Scripting Toolkit which includes the GRUB2 patch to resolve this vulnerability. These new boot images will update GRUB2 and the Forbidden Signature Database (DBX). After the DBX is updated, users will not be able to boot to the older IP, SPP or Scripting ToolKit with Secure Boot enabled. HPE have provided a	N/A	H-HPE-PROL-190820/1286

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			standalone DBX update tool to work with Microsoft Windows, and supported Linux Operating Systems. These tools can be used to update the Forbidden Signature Database (DBX) from within the OS. **Note:** This DBX update mitigates the GRUB2 issue with insmod enabled, and the "Boot Hole" issue for HPE signed GRUB2 applications. **CVE ID : CVE-2020-7205**		
proliant_microserver_gen10					
Improper Control of Generation of Code ('Code Injection')	30-Jul-20	7.2	A potential security vulnerability has been identified in HPE Intelligent Provisioning, Service Pack for ProLiant, and HPE Scripting ToolKit. The vulnerability could be locally exploited to allow arbitrary code execution during the boot process. **Note:** This vulnerability is related to using insmod in GRUB2 in the specific impacted HPE product and HPE is addressing this issue. HPE has made the following software updates and mitigation information to resolve the vulnerability in Intelligent Provisioning, Service Pack for ProLiant, and HPE Scripting ToolKit.	N/A	H-HPE-PROL-190820/1287

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			HPE provided latest Intelligent Provisioning, Service Pack for ProLiant, and HPE Scripting Toolkit which includes the GRUB2 patch to resolve this vulnerability. These new boot images will update GRUB2 and the Forbidden Signature Database (DBX). After the DBX is updated, users will not be able to boot to the older IP, SPP or Scripting ToolKit with Secure Boot enabled. HPE have provided a standalone DBX update tool to work with Microsoft Windows, and supported Linux Operating Systems. These tools can be used to update the Forbidden Signature Database (DBX) from within the OS. **Note:** This DBX update mitigates the GRUB2 issue with insmod enabled, and the "Boot Hole" issue for HPE signed GRUB2 applications. **CVE ID : CVE-2020-7205**		
proliant_microserver_gen10_plus					
Improper Control of Generation of Code ('Code Injection')	30-Jul-20	7.2	A potential security vulnerability has been identified in HPE Intelligent Provisioning, Service Pack for ProLiant, and HPE Scripting ToolKit. The vulnerability could be	N/A	H-HPE-PROL-190820/1288

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			locally exploited to allow arbitrary code execution during the boot process. **Note:** This vulnerability is related to using insmod in GRUB2 in the specific impacted HPE product and HPE is addressing this issue. HPE has made the following software updates and mitigation information to resolve the vulnerability in Intelligent Provisioning, Service Pack for ProLiant, and HPE Scripting ToolKit. HPE provided latest Intelligent Provisioning, Service Pack for ProLiant, and HPE Scripting Toolkit which includes the GRUB2 patch to resolve this vulnerability. These new boot images will update GRUB2 and the Forbidden Signature Database (DBX). After the DBX is updated, users will not be able to boot to the older IP, SPP or Scripting ToolKit with Secure Boot enabled. HPE have provided a standalone DBX update tool to work with Microsoft Windows, and supported Linux Operating Systems. These tools can be used to update the Forbidden Signature Database (DBX) from within the OS. **Note:**		

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			This DBX update mitigates the GRUB2 issue with insmod enabled, and the "Boot Hole" issue for HPE signed GRUB2 applications. **CVE ID : CVE-2020-7205**		
proliant_ml30_gen10_server					
Improper Control of Generation of Code ('Code Injection')	30-Jul-20	7.2	A potential security vulnerability has been identified in HPE Intelligent Provisioning, Service Pack for ProLiant, and HPE Scripting ToolKit. The vulnerability could be locally exploited to allow arbitrary code execution during the boot process. **Note:** This vulnerability is related to using insmod in GRUB2 in the specific impacted HPE product and HPE is addressing this issue. HPE has made the following software updates and mitigation information to resolve the vulnerability in Intelligent Provisioning, Service Pack for ProLiant, and HPE Scripting ToolKit. HPE provided latest Intelligent Provisioning, Service Pack for ProLiant, and HPE Scripting Toolkit which includes the GRUB2 patch to resolve this vulnerability. These new boot images will update GRUB2 and the Forbidden	N/A	H-HPE-PROL-190820/1289

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Signature Database (DBX). After the DBX is updated, users will not be able to boot to the older IP, SPP or Scripting ToolKit with Secure Boot enabled. HPE have provided a standalone DBX update tool to work with Microsoft Windows, and supported Linux Operating Systems. These tools can be used to update the Forbidden Signature Database (DBX) from within the OS. **Note:** This DBX update mitigates the GRUB2 issue with insmod enabled, and the "Boot Hole" issue for HPE signed GRUB2 applications. **CVE ID : CVE-2020-7205**		
proliant_xl220n_gen10_plus_server					
Improper Control of Generation of Code ('Code Injection')	30-Jul-20	7.2	A potential security vulnerability has been identified in HPE Intelligent Provisioning, Service Pack for ProLiant, and HPE Scripting ToolKit. The vulnerability could be locally exploited to allow arbitrary code execution during the boot process. **Note:** This vulnerability is related to using insmod in GRUB2 in the specific impacted HPE product and HPE is addressing this issue. HPE	N/A	H-HPE-PROL-190820/1290

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			has made the following software updates and mitigation information to resolve the vulnerability in Intelligent Provisioning, Service Pack for ProLiant, and HPE Scripting ToolKit. HPE provided latest Intelligent Provisioning, Service Pack for ProLiant, and HPE Scripting Toolkit which includes the GRUB2 patch to resolve this vulnerability. These new boot images will update GRUB2 and the Forbidden Signature Database (DBX). After the DBX is updated, users will not be able to boot to the older IP, SPP or Scripting ToolKit with Secure Boot enabled. HPE have provided a standalone DBX update tool to work with Microsoft Windows, and supported Linux Operating Systems. These tools can be used to update the Forbidden Signature Database (DBX) from within the OS. **Note:** This DBX update mitigates the GRUB2 issue with insmod enabled, and the "Boot Hole" issue for HPE signed GRUB2 applications. **CVE ID : CVE-2020-7205**		
proliant_xl270d_gen9_special_server					

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Improper Control of Generation of Code ('Code Injection')	30-Jul-20	7.2	A potential security vulnerability has been identified in HPE Intelligent Provisioning, Service Pack for ProLiant, and HPE Scripting ToolKit. The vulnerability could be locally exploited to allow arbitrary code execution during the boot process. **Note:** This vulnerability is related to using insmod in GRUB2 in the specific impacted HPE product and HPE is addressing this issue. HPE has made the following software updates and mitigation information to resolve the vulnerability in Intelligent Provisioning, Service Pack for ProLiant, and HPE Scripting ToolKit. HPE provided latest Intelligent Provisioning, Service Pack for ProLiant, and HPE Scripting Toolkit which includes the GRUB2 patch to resolve this vulnerability. These new boot images will update GRUB2 and the Forbidden Signature Database (DBX). After the DBX is updated, users will not be able to boot to the older IP, SPP or Scripting ToolKit with Secure Boot enabled. HPE have provided a standalone DBX update tool to work with	N/A	H-HPE-PROL-190820/1291

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Microsoft Windows, and supported Linux Operating Systems. These tools can be used to update the Forbidden Signature Database (DBX) from within the OS. **Note:** This DBX update mitigates the GRUB2 issue with insmod enabled, and the "Boot Hole" issue for HPE signed GRUB2 applications. **CVE ID : CVE-2020-7205**		
proliant_xl290n_gen10_plus_server					
Improper Control of Generation of Code ('Code Injection')	30-Jul-20	7.2	A potential security vulnerability has been identified in HPE Intelligent Provisioning, Service Pack for ProLiant, and HPE Scripting ToolKit. The vulnerability could be locally exploited to allow arbitrary code execution during the boot process. **Note:** This vulnerability is related to using insmod in GRUB2 in the specific impacted HPE product and HPE is addressing this issue. HPE has made the following software updates and mitigation information to resolve the vulnerability in Intelligent Provisioning, Service Pack for ProLiant, and HPE Scripting ToolKit. HPE provided latest Intelligent Provisioning,	N/A	H-HPE-PROL-190820/1292

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Service Pack for ProLiant, and HPE Scripting Toolkit which includes the GRUB2 patch to resolve this vulnerability. These new boot images will update GRUB2 and the Forbidden Signature Database (DBX). After the DBX is updated, users will not be able to boot to the older IP, SPP or Scripting ToolKit with Secure Boot enabled. HPE have provided a standalone DBX update tool to work with Microsoft Windows, and supported Linux Operating Systems. These tools can be used to update the Forbidden Signature Database (DBX) from within the OS. **Note:** This DBX update mitigates the GRUB2 issue with insmod enabled, and the "Boot Hole" issue for HPE signed GRUB2 applications. **CVE ID : CVE-2020-7205**		
proliant_xl2x260w_gen10_server					
Improper Control of Generation of Code ('Code Injection')	30-Jul-20	7.2	A potential security vulnerability has been identified in HPE Intelligent Provisioning, Service Pack for ProLiant, and HPE Scripting ToolKit. The vulnerability could be locally exploited to allow arbitrary code execution	N/A	H-HPE-PROL-190820/1293

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			during the boot process. **Note:** This vulnerability is related to using insmod in GRUB2 in the specific impacted HPE product and HPE is addressing this issue. HPE has made the following software updates and mitigation information to resolve the vulnerability in Intelligent Provisioning, Service Pack for ProLiant, and HPE Scripting ToolKit. HPE provided latest Intelligent Provisioning, Service Pack for ProLiant, and HPE Scripting Toolkit which includes the GRUB2 patch to resolve this vulnerability. These new boot images will update GRUB2 and the Forbidden Signature Database (DBX). After the DBX is updated, users will not be able to boot to the older IP, SPP or Scripting ToolKit with Secure Boot enabled. HPE have provided a standalone DBX update tool to work with Microsoft Windows, and supported Linux Operating Systems. These tools can be used to update the Forbidden Signature Database (DBX) from within the OS. **Note:** This DBX update mitigates the GRUB2 issue with		

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			insmod enabled, and the "Boot Hole" issue for HPE signed GRUB2 applications. **CVE ID : CVE-2020-7205**		
proliant_xl925g_gen10_plus_1u_4-node_configure-to-order_server					
Improper Control of Generation of Code ('Code Injection')	30-Jul-20	7.2	A potential security vulnerability has been identified in HPE Intelligent Provisioning, Service Pack for ProLiant, and HPE Scripting ToolKit. The vulnerability could be locally exploited to allow arbitrary code execution during the boot process. **Note:** This vulnerability is related to using insmod in GRUB2 in the specific impacted HPE product and HPE is addressing this issue. HPE has made the following software updates and mitigation information to resolve the vulnerability in Intelligent Provisioning, Service Pack for ProLiant, and HPE Scripting ToolKit. HPE provided latest Intelligent Provisioning, Service Pack for ProLiant, and HPE Scripting Toolkit which includes the GRUB2 patch to resolve this vulnerability. These new boot images will update GRUB2 and the Forbidden Signature Database (DBX). After the DBX is updated,	N/A	H-HPE-PROL-190820/1294

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			users will not be able to boot to the older IP, SPP or Scripting ToolKit with Secure Boot enabled. HPE have provided a standalone DBX update tool to work with Microsoft Windows, and supported Linux Operating Systems. These tools can be used to update the Forbidden Signature Database (DBX) from within the OS. **Note:** This DBX update mitigates the GRUB2 issue with insmod enabled, and the "Boot Hole" issue for HPE signed GRUB2 applications. **CVE ID : CVE-2020-7205**		
simplivity_2600_gen10					
Improper Control of Generation of Code ('Code Injection')	30-Jul-20	7.2	A potential security vulnerability has been identified in HPE Intelligent Provisioning, Service Pack for ProLiant, and HPE Scripting ToolKit. The vulnerability could be locally exploited to allow arbitrary code execution during the boot process. **Note:** This vulnerability is related to using insmod in GRUB2 in the specific impacted HPE product and HPE is addressing this issue. HPE has made the following software updates and	N/A	H-HPE-SIMP-190820/1295

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			mitigation information to resolve the vulnerability in Intelligent Provisioning, Service Pack for ProLiant, and HPE Scripting ToolKit. HPE provided latest Intelligent Provisioning, Service Pack for ProLiant, and HPE Scripting Toolkit which includes the GRUB2 patch to resolve this vulnerability. These new boot images will update GRUB2 and the Forbidden Signature Database (DBX). After the DBX is updated, users will not be able to boot to the older IP, SPP or Scripting ToolKit with Secure Boot enabled. HPE have provided a standalone DBX update tool to work with Microsoft Windows, and supported Linux Operating Systems. These tools can be used to update the Forbidden Signature Database (DBX) from within the OS. **Note:** This DBX update mitigates the GRUB2 issue with insmod enabled, and the "Boot Hole" issue for HPE signed GRUB2 applications. **CVE ID : CVE-2020-7205**		
simplivity_325_gen10					
Improper Control of	30-Jul-20	7.2	A potential security vulnerability has been	N/A	H-HPE-SIMP-190820/1296

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Generation of Code ('Code Injection')			identified in HPE Intelligent Provisioning, Service Pack for ProLiant, and HPE Scripting ToolKit. The vulnerability could be locally exploited to allow arbitrary code execution during the boot process. **Note:** This vulnerability is related to using insmod in GRUB2 in the specific impacted HPE product and HPE is addressing this issue. HPE has made the following software updates and mitigation information to resolve the vulnerability in Intelligent Provisioning, Service Pack for ProLiant, and HPE Scripting ToolKit. HPE provided latest Intelligent Provisioning, Service Pack for ProLiant, and HPE Scripting Toolkit which includes the GRUB2 patch to resolve this vulnerability. These new boot images will update GRUB2 and the Forbidden Signature Database (DBX). After the DBX is updated, users will not be able to boot to the older IP, SPP or Scripting ToolKit with Secure Boot enabled. HPE have provided a standalone DBX update tool to work with Microsoft Windows, and supported Linux Operating		

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Systems. These tools can be used to update the Forbidden Signature Database (DBX) from within the OS. **Note:** This DBX update mitigates the GRUB2 issue with insmod enabled, and the "Boot Hole" issue for HPE signed GRUB2 applications. **CVE ID : CVE-2020-7205**		
simplivity_380_gen10					
Improper Control of Generation of Code ('Code Injection')	30-Jul-20	7.2	A potential security vulnerability has been identified in HPE Intelligent Provisioning, Service Pack for ProLiant, and HPE Scripting ToolKit. The vulnerability could be locally exploited to allow arbitrary code execution during the boot process. **Note:** This vulnerability is related to using insmod in GRUB2 in the specific impacted HPE product and HPE is addressing this issue. HPE has made the following software updates and mitigation information to resolve the vulnerability in Intelligent Provisioning, Service Pack for ProLiant, and HPE Scripting ToolKit. HPE provided latest Intelligent Provisioning, Service Pack for ProLiant, and HPE Scripting Toolkit	N/A	H-HPE-SIMP-190820/1297

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			which includes the GRUB2 patch to resolve this vulnerability. These new boot images will update GRUB2 and the Forbidden Signature Database (DBX). After the DBX is updated, users will not be able to boot to the older IP, SPP or Scripting ToolKit with Secure Boot enabled. HPE have provided a standalone DBX update tool to work with Microsoft Windows, and supported Linux Operating Systems. These tools can be used to update the Forbidden Signature Database (DBX) from within the OS. **Note:** This DBX update mitigates the GRUB2 issue with insmod enabled, and the "Boot Hole" issue for HPE signed GRUB2 applications. **CVE ID : CVE-2020-7205**		
storeeasy_1000_storage_gen10					
Improper Control of Generation of Code ('Code Injection')	30-Jul-20	7.2	A potential security vulnerability has been identified in HPE Intelligent Provisioning, Service Pack for ProLiant, and HPE Scripting ToolKit. The vulnerability could be locally exploited to allow arbitrary code execution during the boot process. **Note:** This	N/A	H-HPE-STOR-190820/1298

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			vulnerability is related to using insmod in GRUB2 in the specific impacted HPE product and HPE is addressing this issue. HPE has made the following software updates and mitigation information to resolve the vulnerability in Intelligent Provisioning, Service Pack for ProLiant, and HPE Scripting ToolKit. HPE provided latest Intelligent Provisioning, Service Pack for ProLiant, and HPE Scripting Toolkit which includes the GRUB2 patch to resolve this vulnerability. These new boot images will update GRUB2 and the Forbidden Signature Database (DBX). After the DBX is updated, users will not be able to boot to the older IP, SPP or Scripting ToolKit with Secure Boot enabled. HPE have provided a standalone DBX update tool to work with Microsoft Windows, and supported Linux Operating Systems. These tools can be used to update the Forbidden Signature Database (DBX) from within the OS. **Note:** This DBX update mitigates the GRUB2 issue with insmod enabled, and the "Boot Hole" issue for HPE		

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			signed GRUB2 applications. **CVE ID : CVE-2020-7205**		
synergy_480_gen10_plus_compute_module					
Improper Control of Generation of Code ('Code Injection')	30-Jul-20	7.2	A potential security vulnerability has been identified in HPE Intelligent Provisioning, Service Pack for ProLiant, and HPE Scripting ToolKit. The vulnerability could be locally exploited to allow arbitrary code execution during the boot process. **Note:** This vulnerability is related to using insmod in GRUB2 in the specific impacted HPE product and HPE is addressing this issue. HPE has made the following software updates and mitigation information to resolve the vulnerability in Intelligent Provisioning, Service Pack for ProLiant, and HPE Scripting ToolKit. HPE provided latest Intelligent Provisioning, Service Pack for ProLiant, and HPE Scripting Toolkit which includes the GRUB2 patch to resolve this vulnerability. These new boot images will update GRUB2 and the Forbidden Signature Database (DBX). After the DBX is updated, users will not be able to boot to the older IP, SPP or	N/A	H-HPE-SYNE-190820/1299

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Scripting ToolKit with Secure Boot enabled. HPE have provided a standalone DBX update tool to work with Microsoft Windows, and supported Linux Operating Systems. These tools can be used to update the Forbidden Signature Database (DBX) from within the OS. **Note:** This DBX update mitigates the GRUB2 issue with insmod enabled, and the "Boot Hole" issue for HPE signed GRUB2 applications. **CVE ID : CVE-2020-7205**		
proliant_bl460c_gen9_server_blade					
Improper Control of Generation of Code ('Code Injection')	30-Jul-20	7.2	A potential security vulnerability has been identified in HPE Intelligent Provisioning, Service Pack for ProLiant, and HPE Scripting ToolKit. The vulnerability could be locally exploited to allow arbitrary code execution during the boot process. **Note:** This vulnerability is related to using insmod in GRUB2 in the specific impacted HPE product and HPE is addressing this issue. HPE has made the following software updates and mitigation information to resolve the vulnerability in	N/A	H-HPE-PROL-190820/1300

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Intelligent Provisioning, Service Pack for ProLiant, and HPE Scripting ToolKit. HPE provided latest Intelligent Provisioning, Service Pack for ProLiant, and HPE Scripting Toolkit which includes the GRUB2 patch to resolve this vulnerability. These new boot images will update GRUB2 and the Forbidden Signature Database (DBX). After the DBX is updated, users will not be able to boot to the older IP, SPP or Scripting ToolKit with Secure Boot enabled. HPE have provided a standalone DBX update tool to work with Microsoft Windows, and supported Linux Operating Systems. These tools can be used to update the Forbidden Signature Database (DBX) from within the OS. **Note:** This DBX update mitigates the GRUB2 issue with insmod enabled, and the "Boot Hole" issue for HPE signed GRUB2 applications. **CVE ID : CVE-2020-7205**		
proliant_dl580_gen9_server					
Improper Control of Generation of Code	30-Jul-20	7.2	A potential security vulnerability has been identified in HPE Intelligent Provisioning,	N/A	H-HPE-PROL-190820/1301

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
('Code Injection')			Service Pack for ProLiant, and HPE Scripting ToolKit. The vulnerability could be locally exploited to allow arbitrary code execution during the boot process. **Note:** This vulnerability is related to using insmod in GRUB2 in the specific impacted HPE product and HPE is addressing this issue. HPE has made the following software updates and mitigation information to resolve the vulnerability in Intelligent Provisioning, Service Pack for ProLiant, and HPE Scripting ToolKit. HPE provided latest Intelligent Provisioning, Service Pack for ProLiant, and HPE Scripting Toolkit which includes the GRUB2 patch to resolve this vulnerability. These new boot images will update GRUB2 and the Forbidden Signature Database (DBX). After the DBX is updated, users will not be able to boot to the older IP, SPP or Scripting ToolKit with Secure Boot enabled. HPE have provided a standalone DBX update tool to work with Microsoft Windows, and supported Linux Operating Systems. These tools can be used to update the		

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Forbidden Signature Database (DBX) from within the OS. **Note:** This DBX update mitigates the GRUB2 issue with insmod enabled, and the "Boot Hole" issue for HPE signed GRUB2 applications. **CVE ID : CVE-2020-7205**		
proliant_dl560_gen9_server					
Improper Control of Generation of Code ('Code Injection')	30-Jul-20	7.2	A potential security vulnerability has been identified in HPE Intelligent Provisioning, Service Pack for ProLiant, and HPE Scripting ToolKit. The vulnerability could be locally exploited to allow arbitrary code execution during the boot process. **Note:** This vulnerability is related to using insmod in GRUB2 in the specific impacted HPE product and HPE is addressing this issue. HPE has made the following software updates and mitigation information to resolve the vulnerability in Intelligent Provisioning, Service Pack for ProLiant, and HPE Scripting ToolKit. HPE provided latest Intelligent Provisioning, Service Pack for ProLiant, and HPE Scripting Toolkit which includes the GRUB2 patch to resolve this	N/A	H-HPE-PROL-190820/1302

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			vulnerability. These new boot images will update GRUB2 and the Forbidden Signature Database (DBX). After the DBX is updated, users will not be able to boot to the older IP, SPP or Scripting ToolKit with Secure Boot enabled. HPE have provided a standalone DBX update tool to work with Microsoft Windows, and supported Linux Operating Systems. These tools can be used to update the Forbidden Signature Database (DBX) from within the OS. **Note:** This DBX update mitigates the GRUB2 issue with insmod enabled, and the "Boot Hole" issue for HPE signed GRUB2 applications. **CVE ID : CVE-2020-7205**		
proliant_dl380_gen9_server					
Improper Control of Generation of Code ('Code Injection')	30-Jul-20	7.2	A potential security vulnerability has been identified in HPE Intelligent Provisioning, Service Pack for ProLiant, and HPE Scripting ToolKit. The vulnerability could be locally exploited to allow arbitrary code execution during the boot process. **Note:** This vulnerability is related to using insmod in GRUB2 in	N/A	H-HPE-PROL-190820/1303

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			the specific impacted HPE product and HPE is addressing this issue. HPE has made the following software updates and mitigation information to resolve the vulnerability in Intelligent Provisioning, Service Pack for ProLiant, and HPE Scripting ToolKit. HPE provided latest Intelligent Provisioning, Service Pack for ProLiant, and HPE Scripting Toolkit which includes the GRUB2 patch to resolve this vulnerability. These new boot images will update GRUB2 and the Forbidden Signature Database (DBX). After the DBX is updated, users will not be able to boot to the older IP, SPP or Scripting ToolKit with Secure Boot enabled. HPE have provided a standalone DBX update tool to work with Microsoft Windows, and supported Linux Operating Systems. These tools can be used to update the Forbidden Signature Database (DBX) from within the OS. **Note:** This DBX update mitigates the GRUB2 issue with insmod enabled, and the "Boot Hole" issue for HPE signed GRUB2 applications.		

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2020-7205		
proliant_dl360_gen9_server					
Improper Control of Generation of Code ('Code Injection')	30-Jul-20	7.2	A potential security vulnerability has been identified in HPE Intelligent Provisioning, Service Pack for ProLiant, and HPE Scripting ToolKit. The vulnerability could be locally exploited to allow arbitrary code execution during the boot process. **Note:** This vulnerability is related to using insmod in GRUB2 in the specific impacted HPE product and HPE is addressing this issue. HPE has made the following software updates and mitigation information to resolve the vulnerability in Intelligent Provisioning, Service Pack for ProLiant, and HPE Scripting ToolKit. HPE provided latest Intelligent Provisioning, Service Pack for ProLiant, and HPE Scripting Toolkit which includes the GRUB2 patch to resolve this vulnerability. These new boot images will update GRUB2 and the Forbidden Signature Database (DBX). After the DBX is updated, users will not be able to boot to the older IP, SPP or Scripting ToolKit with Secure Boot enabled. HPE have provided a	N/A	H-HPE-PROL-190820/1304

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			standalone DBX update tool to work with Microsoft Windows, and supported Linux Operating Systems. These tools can be used to update the Forbidden Signature Database (DBX) from within the OS. **Note:** This DBX update mitigates the GRUB2 issue with insmod enabled, and the "Boot Hole" issue for HPE signed GRUB2 applications. **CVE ID : CVE-2020-7205**		
proliant_dl180_gen9_server					
Improper Control of Generation of Code ('Code Injection')	30-Jul-20	7.2	A potential security vulnerability has been identified in HPE Intelligent Provisioning, Service Pack for ProLiant, and HPE Scripting ToolKit. The vulnerability could be locally exploited to allow arbitrary code execution during the boot process. **Note:** This vulnerability is related to using insmod in GRUB2 in the specific impacted HPE product and HPE is addressing this issue. HPE has made the following software updates and mitigation information to resolve the vulnerability in Intelligent Provisioning, Service Pack for ProLiant, and HPE Scripting ToolKit.	N/A	H-HPE-PROL-190820/1305

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			HPE provided latest Intelligent Provisioning, Service Pack for ProLiant, and HPE Scripting Toolkit which includes the GRUB2 patch to resolve this vulnerability. These new boot images will update GRUB2 and the Forbidden Signature Database (DBX). After the DBX is updated, users will not be able to boot to the older IP, SPP or Scripting ToolKit with Secure Boot enabled. HPE have provided a standalone DBX update tool to work with Microsoft Windows, and supported Linux Operating Systems. These tools can be used to update the Forbidden Signature Database (DBX) from within the OS. **Note:** This DBX update mitigates the GRUB2 issue with insmod enabled, and the "Boot Hole" issue for HPE signed GRUB2 applications. **CVE ID : CVE-2020-7205**		
proliant_dl160_gen9_server					
Improper Control of Generation of Code ('Code Injection')	30-Jul-20	7.2	A potential security vulnerability has been identified in HPE Intelligent Provisioning, Service Pack for ProLiant, and HPE Scripting ToolKit. The vulnerability could be	N/A	H-HPE-PROL-190820/1306

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			locally exploited to allow arbitrary code execution during the boot process. **Note:** This vulnerability is related to using insmod in GRUB2 in the specific impacted HPE product and HPE is addressing this issue. HPE has made the following software updates and mitigation information to resolve the vulnerability in Intelligent Provisioning, Service Pack for ProLiant, and HPE Scripting ToolKit. HPE provided latest Intelligent Provisioning, Service Pack for ProLiant, and HPE Scripting Toolkit which includes the GRUB2 patch to resolve this vulnerability. These new boot images will update GRUB2 and the Forbidden Signature Database (DBX). After the DBX is updated, users will not be able to boot to the older IP, SPP or Scripting ToolKit with Secure Boot enabled. HPE have provided a standalone DBX update tool to work with Microsoft Windows, and supported Linux Operating Systems. These tools can be used to update the Forbidden Signature Database (DBX) from within the OS. **Note:**		

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			This DBX update mitigates the GRUB2 issue with insmod enabled, and the "Boot Hole" issue for HPE signed GRUB2 applications. **CVE ID : CVE-2020-7205**		
proliant_dl120_gen9_server					
Improper Control of Generation of Code ('Code Injection')	30-Jul-20	7.2	A potential security vulnerability has been identified in HPE Intelligent Provisioning, Service Pack for ProLiant, and HPE Scripting ToolKit. The vulnerability could be locally exploited to allow arbitrary code execution during the boot process. **Note:** This vulnerability is related to using insmod in GRUB2 in the specific impacted HPE product and HPE is addressing this issue. HPE has made the following software updates and mitigation information to resolve the vulnerability in Intelligent Provisioning, Service Pack for ProLiant, and HPE Scripting ToolKit. HPE provided latest Intelligent Provisioning, Service Pack for ProLiant, and HPE Scripting Toolkit which includes the GRUB2 patch to resolve this vulnerability. These new boot images will update GRUB2 and the Forbidden	N/A	H-HPE-PROL-190820/1307

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Signature Database (DBX). After the DBX is updated, users will not be able to boot to the older IP, SPP or Scripting ToolKit with Secure Boot enabled. HPE have provided a standalone DBX update tool to work with Microsoft Windows, and supported Linux Operating Systems. These tools can be used to update the Forbidden Signature Database (DBX) from within the OS. **Note:** This DBX update mitigates the GRUB2 issue with insmod enabled, and the "Boot Hole" issue for HPE signed GRUB2 applications. **CVE ID : CVE-2020-7205**		
proliant_dl80_gen9_server					
Improper Control of Generation of Code ('Code Injection')	30-Jul-20	7.2	A potential security vulnerability has been identified in HPE Intelligent Provisioning, Service Pack for ProLiant, and HPE Scripting ToolKit. The vulnerability could be locally exploited to allow arbitrary code execution during the boot process. **Note:** This vulnerability is related to using insmod in GRUB2 in the specific impacted HPE product and HPE is addressing this issue. HPE	N/A	H-HPE-PROL-190820/1308

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			has made the following software updates and mitigation information to resolve the vulnerability in Intelligent Provisioning, Service Pack for ProLiant, and HPE Scripting ToolKit. HPE provided latest Intelligent Provisioning, Service Pack for ProLiant, and HPE Scripting Toolkit which includes the GRUB2 patch to resolve this vulnerability. These new boot images will update GRUB2 and the Forbidden Signature Database (DBX). After the DBX is updated, users will not be able to boot to the older IP, SPP or Scripting ToolKit with Secure Boot enabled. HPE have provided a standalone DBX update tool to work with Microsoft Windows, and supported Linux Operating Systems. These tools can be used to update the Forbidden Signature Database (DBX) from within the OS. **Note:** This DBX update mitigates the GRUB2 issue with insmod enabled, and the "Boot Hole" issue for HPE signed GRUB2 applications. **CVE ID : CVE-2020-7205**		
proliant_dl60_gen9_server					

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Improper Control of Generation of Code ('Code Injection')	30-Jul-20	7.2	A potential security vulnerability has been identified in HPE Intelligent Provisioning, Service Pack for ProLiant, and HPE Scripting ToolKit. The vulnerability could be locally exploited to allow arbitrary code execution during the boot process. **Note:** This vulnerability is related to using insmod in GRUB2 in the specific impacted HPE product and HPE is addressing this issue. HPE has made the following software updates and mitigation information to resolve the vulnerability in Intelligent Provisioning, Service Pack for ProLiant, and HPE Scripting ToolKit. HPE provided latest Intelligent Provisioning, Service Pack for ProLiant, and HPE Scripting Toolkit which includes the GRUB2 patch to resolve this vulnerability. These new boot images will update GRUB2 and the Forbidden Signature Database (DBX). After the DBX is updated, users will not be able to boot to the older IP, SPP or Scripting ToolKit with Secure Boot enabled. HPE have provided a standalone DBX update tool to work with	N/A	H-HPE-PROL-190820/1309

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Microsoft Windows, and supported Linux Operating Systems. These tools can be used to update the Forbidden Signature Database (DBX) from within the OS. **Note:** This DBX update mitigates the GRUB2 issue with insmod enabled, and the "Boot Hole" issue for HPE signed GRUB2 applications. **CVE ID : CVE-2020-7205**		
proliant_xl730f_gen9_server					
Improper Control of Generation of Code ('Code Injection')	30-Jul-20	7.2	A potential security vulnerability has been identified in HPE Intelligent Provisioning, Service Pack for ProLiant, and HPE Scripting ToolKit. The vulnerability could be locally exploited to allow arbitrary code execution during the boot process. **Note:** This vulnerability is related to using insmod in GRUB2 in the specific impacted HPE product and HPE is addressing this issue. HPE has made the following software updates and mitigation information to resolve the vulnerability in Intelligent Provisioning, Service Pack for ProLiant, and HPE Scripting ToolKit. HPE provided latest Intelligent Provisioning,	N/A	H-HPE-PROL-190820/1310

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Service Pack for ProLiant, and HPE Scripting Toolkit which includes the GRUB2 patch to resolve this vulnerability. These new boot images will update GRUB2 and the Forbidden Signature Database (DBX). After the DBX is updated, users will not be able to boot to the older IP, SPP or Scripting ToolKit with Secure Boot enabled. HPE have provided a standalone DBX update tool to work with Microsoft Windows, and supported Linux Operating Systems. These tools can be used to update the Forbidden Signature Database (DBX) from within the OS. **Note:** This DBX update mitigates the GRUB2 issue with insmod enabled, and the "Boot Hole" issue for HPE signed GRUB2 applications. **CVE ID : CVE-2020-7205**		
proliant_xl450_gen9_server					
Improper Control of Generation of Code ('Code Injection')	30-Jul-20	7.2	A potential security vulnerability has been identified in HPE Intelligent Provisioning, Service Pack for ProLiant, and HPE Scripting ToolKit. The vulnerability could be locally exploited to allow arbitrary code execution	N/A	H-HPE-PROL-190820/1311

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			during the boot process. **Note:** This vulnerability is related to using insmod in GRUB2 in the specific impacted HPE product and HPE is addressing this issue. HPE has made the following software updates and mitigation information to resolve the vulnerability in Intelligent Provisioning, Service Pack for ProLiant, and HPE Scripting ToolKit. HPE provided latest Intelligent Provisioning, Service Pack for ProLiant, and HPE Scripting Toolkit which includes the GRUB2 patch to resolve this vulnerability. These new boot images will update GRUB2 and the Forbidden Signature Database (DBX). After the DBX is updated, users will not be able to boot to the older IP, SPP or Scripting ToolKit with Secure Boot enabled. HPE have provided a standalone DBX update tool to work with Microsoft Windows, and supported Linux Operating Systems. These tools can be used to update the Forbidden Signature Database (DBX) from within the OS. **Note:** This DBX update mitigates the GRUB2 issue with		

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			insmod enabled, and the "Boot Hole" issue for HPE signed GRUB2 applications. **CVE ID : CVE-2020-7205**		
proliant_xl250a_gen9_server					
Improper Control of Generation of Code ('Code Injection')	30-Jul-20	7.2	A potential security vulnerability has been identified in HPE Intelligent Provisioning, Service Pack for ProLiant, and HPE Scripting ToolKit. The vulnerability could be locally exploited to allow arbitrary code execution during the boot process. **Note:** This vulnerability is related to using insmod in GRUB2 in the specific impacted HPE product and HPE is addressing this issue. HPE has made the following software updates and mitigation information to resolve the vulnerability in Intelligent Provisioning, Service Pack for ProLiant, and HPE Scripting ToolKit. HPE provided latest Intelligent Provisioning, Service Pack for ProLiant, and HPE Scripting Toolkit which includes the GRUB2 patch to resolve this vulnerability. These new boot images will update GRUB2 and the Forbidden Signature Database (DBX). After the DBX is updated,	N/A	H-HPE-PROL-190820/1312

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			users will not be able to boot to the older IP, SPP or Scripting ToolKit with Secure Boot enabled. HPE have provided a standalone DBX update tool to work with Microsoft Windows, and supported Linux Operating Systems. These tools can be used to update the Forbidden Signature Database (DBX) from within the OS. **Note:** This DBX update mitigates the GRUB2 issue with insmod enabled, and the "Boot Hole" issue for HPE signed GRUB2 applications. **CVE ID : CVE-2020-7205**		
proliant_xl230a_gen9_server					
Improper Control of Generation of Code ('Code Injection')	30-Jul-20	7.2	A potential security vulnerability has been identified in HPE Intelligent Provisioning, Service Pack for ProLiant, and HPE Scripting ToolKit. The vulnerability could be locally exploited to allow arbitrary code execution during the boot process. **Note:** This vulnerability is related to using insmod in GRUB2 in the specific impacted HPE product and HPE is addressing this issue. HPE has made the following software updates and	N/A	H-HPE-PROL-190820/1313

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			mitigation information to resolve the vulnerability in Intelligent Provisioning, Service Pack for ProLiant, and HPE Scripting ToolKit. HPE provided latest Intelligent Provisioning, Service Pack for ProLiant, and HPE Scripting Toolkit which includes the GRUB2 patch to resolve this vulnerability. These new boot images will update GRUB2 and the Forbidden Signature Database (DBX). After the DBX is updated, users will not be able to boot to the older IP, SPP or Scripting ToolKit with Secure Boot enabled. HPE have provided a standalone DBX update tool to work with Microsoft Windows, and supported Linux Operating Systems. These tools can be used to update the Forbidden Signature Database (DBX) from within the OS. **Note:** This DBX update mitigates the GRUB2 issue with insmod enabled, and the "Boot Hole" issue for HPE signed GRUB2 applications. **CVE ID : CVE-2020-7205**		
proliant_xl190r_gen9_server					
Improper Control of	30-Jul-20	7.2	A potential security vulnerability has been	N/A	H-HPE-PROL-190820/1314

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Generation of Code ('Code Injection')			identified in HPE Intelligent Provisioning, Service Pack for ProLiant, and HPE Scripting ToolKit. The vulnerability could be locally exploited to allow arbitrary code execution during the boot process. **Note:** This vulnerability is related to using insmod in GRUB2 in the specific impacted HPE product and HPE is addressing this issue. HPE has made the following software updates and mitigation information to resolve the vulnerability in Intelligent Provisioning, Service Pack for ProLiant, and HPE Scripting ToolKit. HPE provided latest Intelligent Provisioning, Service Pack for ProLiant, and HPE Scripting Toolkit which includes the GRUB2 patch to resolve this vulnerability. These new boot images will update GRUB2 and the Forbidden Signature Database (DBX). After the DBX is updated, users will not be able to boot to the older IP, SPP or Scripting ToolKit with Secure Boot enabled. HPE have provided a standalone DBX update tool to work with Microsoft Windows, and supported Linux Operating		

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Systems. These tools can be used to update the Forbidden Signature Database (DBX) from within the OS. **Note:** This DBX update mitigates the GRUB2 issue with insmod enabled, and the "Boot Hole" issue for HPE signed GRUB2 applications. **CVE ID : CVE-2020-7205**		
proliant_xl170r_gen9_server					
Improper Control of Generation of Code ('Code Injection')	30-Jul-20	7.2	A potential security vulnerability has been identified in HPE Intelligent Provisioning, Service Pack for ProLiant, and HPE Scripting ToolKit. The vulnerability could be locally exploited to allow arbitrary code execution during the boot process. **Note:** This vulnerability is related to using insmod in GRUB2 in the specific impacted HPE product and HPE is addressing this issue. HPE has made the following software updates and mitigation information to resolve the vulnerability in Intelligent Provisioning, Service Pack for ProLiant, and HPE Scripting ToolKit. HPE provided latest Intelligent Provisioning, Service Pack for ProLiant, and HPE Scripting Toolkit	N/A	H-HPE-PROL-190820/1315

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			which includes the GRUB2 patch to resolve this vulnerability. These new boot images will update GRUB2 and the Forbidden Signature Database (DBX). After the DBX is updated, users will not be able to boot to the older IP, SPP or Scripting ToolKit with Secure Boot enabled. HPE have provided a standalone DBX update tool to work with Microsoft Windows, and supported Linux Operating Systems. These tools can be used to update the Forbidden Signature Database (DBX) from within the OS. **Note:** This DBX update mitigates the GRUB2 issue with insmod enabled, and the "Boot Hole" issue for HPE signed GRUB2 applications. **CVE ID : CVE-2020-7205**		
synergy_680_gen9_compute_module					
Improper Control of Generation of Code ('Code Injection')	30-Jul-20	7.2	A potential security vulnerability has been identified in HPE Intelligent Provisioning, Service Pack for ProLiant, and HPE Scripting ToolKit. The vulnerability could be locally exploited to allow arbitrary code execution during the boot process. **Note:** This	N/A	H-HPE-SYNE-190820/1316

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			vulnerability is related to using insmod in GRUB2 in the specific impacted HPE product and HPE is addressing this issue. HPE has made the following software updates and mitigation information to resolve the vulnerability in Intelligent Provisioning, Service Pack for ProLiant, and HPE Scripting ToolKit. HPE provided latest Intelligent Provisioning, Service Pack for ProLiant, and HPE Scripting Toolkit which includes the GRUB2 patch to resolve this vulnerability. These new boot images will update GRUB2 and the Forbidden Signature Database (DBX). After the DBX is updated, users will not be able to boot to the older IP, SPP or Scripting ToolKit with Secure Boot enabled. HPE have provided a standalone DBX update tool to work with Microsoft Windows, and supported Linux Operating Systems. These tools can be used to update the Forbidden Signature Database (DBX) from within the OS. **Note:** This DBX update mitigates the GRUB2 issue with insmod enabled, and the "Boot Hole" issue for HPE		

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			signed GRUB2 applications. **CVE ID : CVE-2020-7205**		
synergy_620_gen9_compute_module					
Improper Control of Generation of Code ('Code Injection')	30-Jul-20	7.2	A potential security vulnerability has been identified in HPE Intelligent Provisioning, Service Pack for ProLiant, and HPE Scripting ToolKit. The vulnerability could be locally exploited to allow arbitrary code execution during the boot process. **Note:** This vulnerability is related to using insmod in GRUB2 in the specific impacted HPE product and HPE is addressing this issue. HPE has made the following software updates and mitigation information to resolve the vulnerability in Intelligent Provisioning, Service Pack for ProLiant, and HPE Scripting ToolKit. HPE provided latest Intelligent Provisioning, Service Pack for ProLiant, and HPE Scripting Toolkit which includes the GRUB2 patch to resolve this vulnerability. These new boot images will update GRUB2 and the Forbidden Signature Database (DBX). After the DBX is updated, users will not be able to boot to the older IP, SPP or	N/A	H-HPE-SYNE-190820/1317

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Scripting ToolKit with Secure Boot enabled. HPE have provided a standalone DBX update tool to work with Microsoft Windows, and supported Linux Operating Systems. These tools can be used to update the Forbidden Signature Database (DBX) from within the OS. **Note:** This DBX update mitigates the GRUB2 issue with insmod enabled, and the "Boot Hole" issue for HPE signed GRUB2 applications. **CVE ID : CVE-2020-7205**		
synergy_480_gen9_compute_module					
Improper Control of Generation of Code ('Code Injection')	30-Jul-20	7.2	A potential security vulnerability has been identified in HPE Intelligent Provisioning, Service Pack for ProLiant, and HPE Scripting ToolKit. The vulnerability could be locally exploited to allow arbitrary code execution during the boot process. **Note:** This vulnerability is related to using insmod in GRUB2 in the specific impacted HPE product and HPE is addressing this issue. HPE has made the following software updates and mitigation information to resolve the vulnerability in	N/A	H-HPE-SYNE-190820/1318

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Intelligent Provisioning, Service Pack for ProLiant, and HPE Scripting ToolKit. HPE provided latest Intelligent Provisioning, Service Pack for ProLiant, and HPE Scripting Toolkit which includes the GRUB2 patch to resolve this vulnerability. These new boot images will update GRUB2 and the Forbidden Signature Database (DBX). After the DBX is updated, users will not be able to boot to the older IP, SPP or Scripting ToolKit with Secure Boot enabled. HPE have provided a standalone DBX update tool to work with Microsoft Windows, and supported Linux Operating Systems. These tools can be used to update the Forbidden Signature Database (DBX) from within the OS. **Note:** This DBX update mitigates the GRUB2 issue with insmod enabled, and the "Boot Hole" issue for HPE signed GRUB2 applications. **CVE ID : CVE-2020-7205**		
proliant_ml150_gen9_server					
Improper Control of Generation of Code	30-Jul-20	7.2	A potential security vulnerability has been identified in HPE Intelligent Provisioning,	N/A	H-HPE-PROL-190820/1319

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
('Code Injection')			Service Pack for ProLiant, and HPE Scripting ToolKit. The vulnerability could be locally exploited to allow arbitrary code execution during the boot process. **Note:** This vulnerability is related to using insmod in GRUB2 in the specific impacted HPE product and HPE is addressing this issue. HPE has made the following software updates and mitigation information to resolve the vulnerability in Intelligent Provisioning, Service Pack for ProLiant, and HPE Scripting ToolKit. HPE provided latest Intelligent Provisioning, Service Pack for ProLiant, and HPE Scripting Toolkit which includes the GRUB2 patch to resolve this vulnerability. These new boot images will update GRUB2 and the Forbidden Signature Database (DBX). After the DBX is updated, users will not be able to boot to the older IP, SPP or Scripting ToolKit with Secure Boot enabled. HPE have provided a standalone DBX update tool to work with Microsoft Windows, and supported Linux Operating Systems. These tools can be used to update the		

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Forbidden Signature Database (DBX) from within the OS. **Note:** This DBX update mitigates the GRUB2 issue with insmod enabled, and the "Boot Hole" issue for HPE signed GRUB2 applications. **CVE ID : CVE-2020-7205**		
proliant_ml110_gen9_server					
Improper Control of Generation of Code ('Code Injection')	30-Jul-20	7.2	A potential security vulnerability has been identified in HPE Intelligent Provisioning, Service Pack for ProLiant, and HPE Scripting ToolKit. The vulnerability could be locally exploited to allow arbitrary code execution during the boot process. **Note:** This vulnerability is related to using insmod in GRUB2 in the specific impacted HPE product and HPE is addressing this issue. HPE has made the following software updates and mitigation information to resolve the vulnerability in Intelligent Provisioning, Service Pack for ProLiant, and HPE Scripting ToolKit. HPE provided latest Intelligent Provisioning, Service Pack for ProLiant, and HPE Scripting Toolkit which includes the GRUB2 patch to resolve this	N/A	H-HPE-PROL-190820/1320

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			vulnerability. These new boot images will update GRUB2 and the Forbidden Signature Database (DBX). After the DBX is updated, users will not be able to boot to the older IP, SPP or Scripting ToolKit with Secure Boot enabled. HPE have provided a standalone DBX update tool to work with Microsoft Windows, and supported Linux Operating Systems. These tools can be used to update the Forbidden Signature Database (DBX) from within the OS. **Note:** This DBX update mitigates the GRUB2 issue with insmod enabled, and the "Boot Hole" issue for HPE signed GRUB2 applications. **CVE ID : CVE-2020-7205**		
apollo_4200_gen9_server					
Improper Control of Generation of Code ('Code Injection')	30-Jul-20	7.2	A potential security vulnerability has been identified in HPE Intelligent Provisioning, Service Pack for ProLiant, and HPE Scripting ToolKit. The vulnerability could be locally exploited to allow arbitrary code execution during the boot process. **Note:** This vulnerability is related to using insmod in GRUB2 in	N/A	H-HPE-APOL-190820/1321

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			the specific impacted HPE product and HPE is addressing this issue. HPE has made the following software updates and mitigation information to resolve the vulnerability in Intelligent Provisioning, Service Pack for ProLiant, and HPE Scripting ToolKit. HPE provided latest Intelligent Provisioning, Service Pack for ProLiant, and HPE Scripting Toolkit which includes the GRUB2 patch to resolve this vulnerability. These new boot images will update GRUB2 and the Forbidden Signature Database (DBX). After the DBX is updated, users will not be able to boot to the older IP, SPP or Scripting ToolKit with Secure Boot enabled. HPE have provided a standalone DBX update tool to work with Microsoft Windows, and supported Linux Operating Systems. These tools can be used to update the Forbidden Signature Database (DBX) from within the OS. **Note:** This DBX update mitigates the GRUB2 issue with insmod enabled, and the "Boot Hole" issue for HPE signed GRUB2 applications.		

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2020-7205		
proliant_ml350_gen9_server					
Improper Control of Generation of Code ('Code Injection')	30-Jul-20	7.2	A potential security vulnerability has been identified in HPE Intelligent Provisioning, Service Pack for ProLiant, and HPE Scripting ToolKit. The vulnerability could be locally exploited to allow arbitrary code execution during the boot process. **Note:** This vulnerability is related to using insmod in GRUB2 in the specific impacted HPE product and HPE is addressing this issue. HPE has made the following software updates and mitigation information to resolve the vulnerability in Intelligent Provisioning, Service Pack for ProLiant, and HPE Scripting ToolKit. HPE provided latest Intelligent Provisioning, Service Pack for ProLiant, and HPE Scripting Toolkit which includes the GRUB2 patch to resolve this vulnerability. These new boot images will update GRUB2 and the Forbidden Signature Database (DBX). After the DBX is updated, users will not be able to boot to the older IP, SPP or Scripting ToolKit with Secure Boot enabled. HPE have provided a	N/A	H-HPE-PROL-190820/1322

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			standalone DBX update tool to work with Microsoft Windows, and supported Linux Operating Systems. These tools can be used to update the Forbidden Signature Database (DBX) from within the OS. **Note:** This DBX update mitigates the GRUB2 issue with insmod enabled, and the "Boot Hole" issue for HPE signed GRUB2 applications. **CVE ID : CVE-2020-7205**		
proliant_ws460c_gen9_graphics_server_blade					
Improper Control of Generation of Code ('Code Injection')	30-Jul-20	7.2	A potential security vulnerability has been identified in HPE Intelligent Provisioning, Service Pack for ProLiant, and HPE Scripting ToolKit. The vulnerability could be locally exploited to allow arbitrary code execution during the boot process. **Note:** This vulnerability is related to using insmod in GRUB2 in the specific impacted HPE product and HPE is addressing this issue. HPE has made the following software updates and mitigation information to resolve the vulnerability in Intelligent Provisioning, Service Pack for ProLiant, and HPE Scripting ToolKit.	N/A	H-HPE-PROL-190820/1323

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			HPE provided latest Intelligent Provisioning, Service Pack for ProLiant, and HPE Scripting Toolkit which includes the GRUB2 patch to resolve this vulnerability. These new boot images will update GRUB2 and the Forbidden Signature Database (DBX). After the DBX is updated, users will not be able to boot to the older IP, SPP or Scripting ToolKit with Secure Boot enabled. HPE have provided a standalone DBX update tool to work with Microsoft Windows, and supported Linux Operating Systems. These tools can be used to update the Forbidden Signature Database (DBX) from within the OS. **Note:** This DBX update mitigates the GRUB2 issue with insmod enabled, and the "Boot Hole" issue for HPE signed GRUB2 applications. **CVE ID : CVE-2020-7205**		
apollo_4200_gen10_server					
Improper Control of Generation of Code ('Code Injection')	30-Jul-20	7.2	A potential security vulnerability has been identified in HPE Intelligent Provisioning, Service Pack for ProLiant, and HPE Scripting ToolKit. The vulnerability could be	N/A	H-HPE-APOL-190820/1324

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			locally exploited to allow arbitrary code execution during the boot process. **Note:** This vulnerability is related to using insmod in GRUB2 in the specific impacted HPE product and HPE is addressing this issue. HPE has made the following software updates and mitigation information to resolve the vulnerability in Intelligent Provisioning, Service Pack for ProLiant, and HPE Scripting ToolKit. HPE provided latest Intelligent Provisioning, Service Pack for ProLiant, and HPE Scripting Toolkit which includes the GRUB2 patch to resolve this vulnerability. These new boot images will update GRUB2 and the Forbidden Signature Database (DBX). After the DBX is updated, users will not be able to boot to the older IP, SPP or Scripting ToolKit with Secure Boot enabled. HPE have provided a standalone DBX update tool to work with Microsoft Windows, and supported Linux Operating Systems. These tools can be used to update the Forbidden Signature Database (DBX) from within the OS. **Note:**		

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			This DBX update mitigates the GRUB2 issue with insmod enabled, and the "Boot Hole" issue for HPE signed GRUB2 applications. **CVE ID : CVE-2020-7205**		
proliant_bl460c_gen10_server_blade					
Improper Control of Generation of Code ('Code Injection')	30-Jul-20	7.2	A potential security vulnerability has been identified in HPE Intelligent Provisioning, Service Pack for ProLiant, and HPE Scripting ToolKit. The vulnerability could be locally exploited to allow arbitrary code execution during the boot process. **Note:** This vulnerability is related to using insmod in GRUB2 in the specific impacted HPE product and HPE is addressing this issue. HPE has made the following software updates and mitigation information to resolve the vulnerability in Intelligent Provisioning, Service Pack for ProLiant, and HPE Scripting ToolKit. HPE provided latest Intelligent Provisioning, Service Pack for ProLiant, and HPE Scripting Toolkit which includes the GRUB2 patch to resolve this vulnerability. These new boot images will update GRUB2 and the Forbidden	N/A	H-HPE-PROL-190820/1325

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Signature Database (DBX). After the DBX is updated, users will not be able to boot to the older IP, SPP or Scripting ToolKit with Secure Boot enabled. HPE have provided a standalone DBX update tool to work with Microsoft Windows, and supported Linux Operating Systems. These tools can be used to update the Forbidden Signature Database (DBX) from within the OS. **Note:** This DBX update mitigates the GRUB2 issue with insmod enabled, and the "Boot Hole" issue for HPE signed GRUB2 applications. **CVE ID : CVE-2020-7205**		
proliant_dl580_gen10_server					
Improper Control of Generation of Code ('Code Injection')	30-Jul-20	7.2	A potential security vulnerability has been identified in HPE Intelligent Provisioning, Service Pack for ProLiant, and HPE Scripting ToolKit. The vulnerability could be locally exploited to allow arbitrary code execution during the boot process. **Note:** This vulnerability is related to using insmod in GRUB2 in the specific impacted HPE product and HPE is addressing this issue. HPE	N/A	H-HPE-PROL-190820/1326

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			has made the following software updates and mitigation information to resolve the vulnerability in Intelligent Provisioning, Service Pack for ProLiant, and HPE Scripting ToolKit. HPE provided latest Intelligent Provisioning, Service Pack for ProLiant, and HPE Scripting Toolkit which includes the GRUB2 patch to resolve this vulnerability. These new boot images will update GRUB2 and the Forbidden Signature Database (DBX). After the DBX is updated, users will not be able to boot to the older IP, SPP or Scripting ToolKit with Secure Boot enabled. HPE have provided a standalone DBX update tool to work with Microsoft Windows, and supported Linux Operating Systems. These tools can be used to update the Forbidden Signature Database (DBX) from within the OS. **Note:** This DBX update mitigates the GRUB2 issue with insmod enabled, and the "Boot Hole" issue for HPE signed GRUB2 applications. **CVE ID : CVE-2020-7205**		
proliant_dl560_gen10_server					

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Improper Control of Generation of Code ('Code Injection')	30-Jul-20	7.2	A potential security vulnerability has been identified in HPE Intelligent Provisioning, Service Pack for ProLiant, and HPE Scripting ToolKit. The vulnerability could be locally exploited to allow arbitrary code execution during the boot process. **Note:** This vulnerability is related to using insmod in GRUB2 in the specific impacted HPE product and HPE is addressing this issue. HPE has made the following software updates and mitigation information to resolve the vulnerability in Intelligent Provisioning, Service Pack for ProLiant, and HPE Scripting ToolKit. HPE provided latest Intelligent Provisioning, Service Pack for ProLiant, and HPE Scripting Toolkit which includes the GRUB2 patch to resolve this vulnerability. These new boot images will update GRUB2 and the Forbidden Signature Database (DBX). After the DBX is updated, users will not be able to boot to the older IP, SPP or Scripting ToolKit with Secure Boot enabled. HPE have provided a standalone DBX update tool to work with	N/A	H-HPE-PROL-190820/1327

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Microsoft Windows, and supported Linux Operating Systems. These tools can be used to update the Forbidden Signature Database (DBX) from within the OS. **Note:** This DBX update mitigates the GRUB2 issue with insmod enabled, and the "Boot Hole" issue for HPE signed GRUB2 applications. **CVE ID : CVE-2020-7205**		
proliant_dl380_gen10_server					
Improper Control of Generation of Code ('Code Injection')	30-Jul-20	7.2	A potential security vulnerability has been identified in HPE Intelligent Provisioning, Service Pack for ProLiant, and HPE Scripting ToolKit. The vulnerability could be locally exploited to allow arbitrary code execution during the boot process. **Note:** This vulnerability is related to using insmod in GRUB2 in the specific impacted HPE product and HPE is addressing this issue. HPE has made the following software updates and mitigation information to resolve the vulnerability in Intelligent Provisioning, Service Pack for ProLiant, and HPE Scripting ToolKit. HPE provided latest Intelligent Provisioning,	N/A	H-HPE-PROL-190820/1328

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Service Pack for ProLiant, and HPE Scripting Toolkit which includes the GRUB2 patch to resolve this vulnerability. These new boot images will update GRUB2 and the Forbidden Signature Database (DBX). After the DBX is updated, users will not be able to boot to the older IP, SPP or Scripting ToolKit with Secure Boot enabled. HPE have provided a standalone DBX update tool to work with Microsoft Windows, and supported Linux Operating Systems. These tools can be used to update the Forbidden Signature Database (DBX) from within the OS. **Note:** This DBX update mitigates the GRUB2 issue with insmod enabled, and the "Boot Hole" issue for HPE signed GRUB2 applications. **CVE ID : CVE-2020-7205**		
proliant_dl360_gen10_server					
Improper Control of Generation of Code ('Code Injection')	30-Jul-20	7.2	A potential security vulnerability has been identified in HPE Intelligent Provisioning, Service Pack for ProLiant, and HPE Scripting ToolKit. The vulnerability could be locally exploited to allow arbitrary code execution	N/A	H-HPE-PROL-190820/1329

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			during the boot process. **Note:** This vulnerability is related to using insmod in GRUB2 in the specific impacted HPE product and HPE is addressing this issue. HPE has made the following software updates and mitigation information to resolve the vulnerability in Intelligent Provisioning, Service Pack for ProLiant, and HPE Scripting ToolKit. HPE provided latest Intelligent Provisioning, Service Pack for ProLiant, and HPE Scripting Toolkit which includes the GRUB2 patch to resolve this vulnerability. These new boot images will update GRUB2 and the Forbidden Signature Database (DBX). After the DBX is updated, users will not be able to boot to the older IP, SPP or Scripting ToolKit with Secure Boot enabled. HPE have provided a standalone DBX update tool to work with Microsoft Windows, and supported Linux Operating Systems. These tools can be used to update the Forbidden Signature Database (DBX) from within the OS. **Note:** This DBX update mitigates the GRUB2 issue with		

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			insmod enabled, and the "Boot Hole" issue for HPE signed GRUB2 applications. **CVE ID : CVE-2020-7205**		
proliant_dl180_gen10_server					
Improper Control of Generation of Code ('Code Injection')	30-Jul-20	7.2	A potential security vulnerability has been identified in HPE Intelligent Provisioning, Service Pack for ProLiant, and HPE Scripting ToolKit. The vulnerability could be locally exploited to allow arbitrary code execution during the boot process. **Note:** This vulnerability is related to using insmod in GRUB2 in the specific impacted HPE product and HPE is addressing this issue. HPE has made the following software updates and mitigation information to resolve the vulnerability in Intelligent Provisioning, Service Pack for ProLiant, and HPE Scripting ToolKit. HPE provided latest Intelligent Provisioning, Service Pack for ProLiant, and HPE Scripting Toolkit which includes the GRUB2 patch to resolve this vulnerability. These new boot images will update GRUB2 and the Forbidden Signature Database (DBX). After the DBX is updated,	N/A	H-HPE-PROL-190820/1330

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			users will not be able to boot to the older IP, SPP or Scripting ToolKit with Secure Boot enabled. HPE have provided a standalone DBX update tool to work with Microsoft Windows, and supported Linux Operating Systems. These tools can be used to update the Forbidden Signature Database (DBX) from within the OS. **Note:** This DBX update mitigates the GRUB2 issue with insmod enabled, and the "Boot Hole" issue for HPE signed GRUB2 applications. **CVE ID : CVE-2020-7205**		
proliant_dl160_gen10_server					
Improper Control of Generation of Code ('Code Injection')	30-Jul-20	7.2	A potential security vulnerability has been identified in HPE Intelligent Provisioning, Service Pack for ProLiant, and HPE Scripting ToolKit. The vulnerability could be locally exploited to allow arbitrary code execution during the boot process. **Note:** This vulnerability is related to using insmod in GRUB2 in the specific impacted HPE product and HPE is addressing this issue. HPE has made the following software updates and	N/A	H-HPE-PROL-190820/1331

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			mitigation information to resolve the vulnerability in Intelligent Provisioning, Service Pack for ProLiant, and HPE Scripting ToolKit. HPE provided latest Intelligent Provisioning, Service Pack for ProLiant, and HPE Scripting Toolkit which includes the GRUB2 patch to resolve this vulnerability. These new boot images will update GRUB2 and the Forbidden Signature Database (DBX). After the DBX is updated, users will not be able to boot to the older IP, SPP or Scripting ToolKit with Secure Boot enabled. HPE have provided a standalone DBX update tool to work with Microsoft Windows, and supported Linux Operating Systems. These tools can be used to update the Forbidden Signature Database (DBX) from within the OS. **Note:** This DBX update mitigates the GRUB2 issue with insmod enabled, and the "Boot Hole" issue for HPE signed GRUB2 applications. **CVE ID : CVE-2020-7205**		
proliant_dl120_gen10_server					
Improper Control of	30-Jul-20	7.2	A potential security vulnerability has been	N/A	H-HPE-PROL-190820/1332

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Generation of Code ('Code Injection')			identified in HPE Intelligent Provisioning, Service Pack for ProLiant, and HPE Scripting ToolKit. The vulnerability could be locally exploited to allow arbitrary code execution during the boot process. **Note:** This vulnerability is related to using insmod in GRUB2 in the specific impacted HPE product and HPE is addressing this issue. HPE has made the following software updates and mitigation information to resolve the vulnerability in Intelligent Provisioning, Service Pack for ProLiant, and HPE Scripting ToolKit. HPE provided latest Intelligent Provisioning, Service Pack for ProLiant, and HPE Scripting Toolkit which includes the GRUB2 patch to resolve this vulnerability. These new boot images will update GRUB2 and the Forbidden Signature Database (DBX). After the DBX is updated, users will not be able to boot to the older IP, SPP or Scripting ToolKit with Secure Boot enabled. HPE have provided a standalone DBX update tool to work with Microsoft Windows, and supported Linux Operating		

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Systems. These tools can be used to update the Forbidden Signature Database (DBX) from within the OS. **Note:** This DBX update mitigates the GRUB2 issue with insmod enabled, and the "Boot Hole" issue for HPE signed GRUB2 applications. **CVE ID : CVE-2020-7205**		
proliant_ml350_gen10_server					
Improper Control of Generation of Code ('Code Injection')	30-Jul-20	7.2	A potential security vulnerability has been identified in HPE Intelligent Provisioning, Service Pack for ProLiant, and HPE Scripting ToolKit. The vulnerability could be locally exploited to allow arbitrary code execution during the boot process. **Note:** This vulnerability is related to using insmod in GRUB2 in the specific impacted HPE product and HPE is addressing this issue. HPE has made the following software updates and mitigation information to resolve the vulnerability in Intelligent Provisioning, Service Pack for ProLiant, and HPE Scripting ToolKit. HPE provided latest Intelligent Provisioning, Service Pack for ProLiant, and HPE Scripting Toolkit	N/A	H-HPE-PROL-190820/1333

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			which includes the GRUB2 patch to resolve this vulnerability. These new boot images will update GRUB2 and the Forbidden Signature Database (DBX). After the DBX is updated, users will not be able to boot to the older IP, SPP or Scripting ToolKit with Secure Boot enabled. HPE have provided a standalone DBX update tool to work with Microsoft Windows, and supported Linux Operating Systems. These tools can be used to update the Forbidden Signature Database (DBX) from within the OS. **Note:** This DBX update mitigates the GRUB2 issue with insmod enabled, and the "Boot Hole" issue for HPE signed GRUB2 applications. **CVE ID : CVE-2020-7205**		
proliant_ml110_gen10_server					
Improper Control of Generation of Code ('Code Injection')	30-Jul-20	7.2	A potential security vulnerability has been identified in HPE Intelligent Provisioning, Service Pack for ProLiant, and HPE Scripting ToolKit. The vulnerability could be locally exploited to allow arbitrary code execution during the boot process. **Note:** This	N/A	H-HPE-PROL-190820/1334

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			vulnerability is related to using insmod in GRUB2 in the specific impacted HPE product and HPE is addressing this issue. HPE has made the following software updates and mitigation information to resolve the vulnerability in Intelligent Provisioning, Service Pack for ProLiant, and HPE Scripting ToolKit. HPE provided latest Intelligent Provisioning, Service Pack for ProLiant, and HPE Scripting Toolkit which includes the GRUB2 patch to resolve this vulnerability. These new boot images will update GRUB2 and the Forbidden Signature Database (DBX). After the DBX is updated, users will not be able to boot to the older IP, SPP or Scripting ToolKit with Secure Boot enabled. HPE have provided a standalone DBX update tool to work with Microsoft Windows, and supported Linux Operating Systems. These tools can be used to update the Forbidden Signature Database (DBX) from within the OS. **Note:** This DBX update mitigates the GRUB2 issue with insmod enabled, and the "Boot Hole" issue for HPE		

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			signed GRUB2 applications. **CVE ID : CVE-2020-7205**		
proliant_xl450_gen10_server					
Improper Control of Generation of Code ('Code Injection')	30-Jul-20	7.2	A potential security vulnerability has been identified in HPE Intelligent Provisioning, Service Pack for ProLiant, and HPE Scripting ToolKit. The vulnerability could be locally exploited to allow arbitrary code execution during the boot process. **Note:** This vulnerability is related to using insmod in GRUB2 in the specific impacted HPE product and HPE is addressing this issue. HPE has made the following software updates and mitigation information to resolve the vulnerability in Intelligent Provisioning, Service Pack for ProLiant, and HPE Scripting ToolKit. HPE provided latest Intelligent Provisioning, Service Pack for ProLiant, and HPE Scripting Toolkit which includes the GRUB2 patch to resolve this vulnerability. These new boot images will update GRUB2 and the Forbidden Signature Database (DBX). After the DBX is updated, users will not be able to boot to the older IP, SPP or	N/A	H-HPE-PROL-190820/1335

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Scripting ToolKit with Secure Boot enabled. HPE have provided a standalone DBX update tool to work with Microsoft Windows, and supported Linux Operating Systems. These tools can be used to update the Forbidden Signature Database (DBX) from within the OS. **Note:** This DBX update mitigates the GRUB2 issue with insmod enabled, and the "Boot Hole" issue for HPE signed GRUB2 applications. **CVE ID : CVE-2020-7205**		
proliant_xl270d_gen10_server					
Improper Control of Generation of Code ('Code Injection')	30-Jul-20	7.2	A potential security vulnerability has been identified in HPE Intelligent Provisioning, Service Pack for ProLiant, and HPE Scripting ToolKit. The vulnerability could be locally exploited to allow arbitrary code execution during the boot process. **Note:** This vulnerability is related to using insmod in GRUB2 in the specific impacted HPE product and HPE is addressing this issue. HPE has made the following software updates and mitigation information to resolve the vulnerability in	N/A	H-HPE-PROL-190820/1336

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Intelligent Provisioning, Service Pack for ProLiant, and HPE Scripting ToolKit. HPE provided latest Intelligent Provisioning, Service Pack for ProLiant, and HPE Scripting Toolkit which includes the GRUB2 patch to resolve this vulnerability. These new boot images will update GRUB2 and the Forbidden Signature Database (DBX). After the DBX is updated, users will not be able to boot to the older IP, SPP or Scripting ToolKit with Secure Boot enabled. HPE have provided a standalone DBX update tool to work with Microsoft Windows, and supported Linux Operating Systems. These tools can be used to update the Forbidden Signature Database (DBX) from within the OS. **Note:** This DBX update mitigates the GRUB2 issue with insmod enabled, and the "Boot Hole" issue for HPE signed GRUB2 applications. **CVE ID : CVE-2020-7205**		
proliant_xl230k_gen10_server					
Improper Control of Generation of Code	30-Jul-20	7.2	A potential security vulnerability has been identified in HPE Intelligent Provisioning,	N/A	H-HPE-PROL-190820/1337

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
('Code Injection')			Service Pack for ProLiant, and HPE Scripting ToolKit. The vulnerability could be locally exploited to allow arbitrary code execution during the boot process. **Note:** This vulnerability is related to using insmod in GRUB2 in the specific impacted HPE product and HPE is addressing this issue. HPE has made the following software updates and mitigation information to resolve the vulnerability in Intelligent Provisioning, Service Pack for ProLiant, and HPE Scripting ToolKit. HPE provided latest Intelligent Provisioning, Service Pack for ProLiant, and HPE Scripting Toolkit which includes the GRUB2 patch to resolve this vulnerability. These new boot images will update GRUB2 and the Forbidden Signature Database (DBX). After the DBX is updated, users will not be able to boot to the older IP, SPP or Scripting ToolKit with Secure Boot enabled. HPE have provided a standalone DBX update tool to work with Microsoft Windows, and supported Linux Operating Systems. These tools can be used to update the		

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Forbidden Signature Database (DBX) from within the OS. **Note:** This DBX update mitigates the GRUB2 issue with insmod enabled, and the "Boot Hole" issue for HPE signed GRUB2 applications. **CVE ID : CVE-2020-7205**		
proliant_xl190r_gen10_server					
Improper Control of Generation of Code ('Code Injection')	30-Jul-20	7.2	A potential security vulnerability has been identified in HPE Intelligent Provisioning, Service Pack for ProLiant, and HPE Scripting ToolKit. The vulnerability could be locally exploited to allow arbitrary code execution during the boot process. **Note:** This vulnerability is related to using insmod in GRUB2 in the specific impacted HPE product and HPE is addressing this issue. HPE has made the following software updates and mitigation information to resolve the vulnerability in Intelligent Provisioning, Service Pack for ProLiant, and HPE Scripting ToolKit. HPE provided latest Intelligent Provisioning, Service Pack for ProLiant, and HPE Scripting Toolkit which includes the GRUB2 patch to resolve this	N/A	H-HPE-PROL-190820/1338

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			vulnerability. These new boot images will update GRUB2 and the Forbidden Signature Database (DBX). After the DBX is updated, users will not be able to boot to the older IP, SPP or Scripting ToolKit with Secure Boot enabled. HPE have provided a standalone DBX update tool to work with Microsoft Windows, and supported Linux Operating Systems. These tools can be used to update the Forbidden Signature Database (DBX) from within the OS. **Note:** This DBX update mitigates the GRUB2 issue with insmod enabled, and the "Boot Hole" issue for HPE signed GRUB2 applications. **CVE ID : CVE-2020-7205**		
proliant_xl170r_gen10_server					
Improper Control of Generation of Code ('Code Injection')	30-Jul-20	7.2	A potential security vulnerability has been identified in HPE Intelligent Provisioning, Service Pack for ProLiant, and HPE Scripting ToolKit. The vulnerability could be locally exploited to allow arbitrary code execution during the boot process. **Note:** This vulnerability is related to using insmod in GRUB2 in	N/A	H-HPE-PROL-190820/1339

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			the specific impacted HPE product and HPE is addressing this issue. HPE has made the following software updates and mitigation information to resolve the vulnerability in Intelligent Provisioning, Service Pack for ProLiant, and HPE Scripting ToolKit. HPE provided latest Intelligent Provisioning, Service Pack for ProLiant, and HPE Scripting Toolkit which includes the GRUB2 patch to resolve this vulnerability. These new boot images will update GRUB2 and the Forbidden Signature Database (DBX). After the DBX is updated, users will not be able to boot to the older IP, SPP or Scripting ToolKit with Secure Boot enabled. HPE have provided a standalone DBX update tool to work with Microsoft Windows, and supported Linux Operating Systems. These tools can be used to update the Forbidden Signature Database (DBX) from within the OS. **Note:** This DBX update mitigates the GRUB2 issue with insmod enabled, and the "Boot Hole" issue for HPE signed GRUB2 applications.		

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2020-7205		
proliant_e910_server_blade					
Improper Control of Generation of Code ('Code Injection')	30-Jul-20	7.2	A potential security vulnerability has been identified in HPE Intelligent Provisioning, Service Pack for ProLiant, and HPE Scripting ToolKit. The vulnerability could be locally exploited to allow arbitrary code execution during the boot process. **Note:** This vulnerability is related to using insmod in GRUB2 in the specific impacted HPE product and HPE is addressing this issue. HPE has made the following software updates and mitigation information to resolve the vulnerability in Intelligent Provisioning, Service Pack for ProLiant, and HPE Scripting ToolKit. HPE provided latest Intelligent Provisioning, Service Pack for ProLiant, and HPE Scripting Toolkit which includes the GRUB2 patch to resolve this vulnerability. These new boot images will update GRUB2 and the Forbidden Signature Database (DBX). After the DBX is updated, users will not be able to boot to the older IP, SPP or Scripting ToolKit with Secure Boot enabled. HPE have provided a	N/A	H-HPE-PROL-190820/1340

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			standalone DBX update tool to work with Microsoft Windows, and supported Linux Operating Systems. These tools can be used to update the Forbidden Signature Database (DBX) from within the OS. **Note:** This DBX update mitigates the GRUB2 issue with insmod enabled, and the "Boot Hole" issue for HPE signed GRUB2 applications. **CVE ID : CVE-2020-7205**		
synergy_660_gen10_compute_module					
Improper Control of Generation of Code ('Code Injection')	30-Jul-20	7.2	A potential security vulnerability has been identified in HPE Intelligent Provisioning, Service Pack for ProLiant, and HPE Scripting ToolKit. The vulnerability could be locally exploited to allow arbitrary code execution during the boot process. **Note:** This vulnerability is related to using insmod in GRUB2 in the specific impacted HPE product and HPE is addressing this issue. HPE has made the following software updates and mitigation information to resolve the vulnerability in Intelligent Provisioning, Service Pack for ProLiant, and HPE Scripting ToolKit.	N/A	H-HPE-SYNE-190820/1341

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			HPE provided latest Intelligent Provisioning, Service Pack for ProLiant, and HPE Scripting Toolkit which includes the GRUB2 patch to resolve this vulnerability. These new boot images will update GRUB2 and the Forbidden Signature Database (DBX). After the DBX is updated, users will not be able to boot to the older IP, SPP or Scripting ToolKit with Secure Boot enabled. HPE have provided a standalone DBX update tool to work with Microsoft Windows, and supported Linux Operating Systems. These tools can be used to update the Forbidden Signature Database (DBX) from within the OS. **Note:** This DBX update mitigates the GRUB2 issue with insmod enabled, and the "Boot Hole" issue for HPE signed GRUB2 applications. **CVE ID : CVE-2020-7205**		
synergy_480_gen10_compute_module					
Improper Control of Generation of Code ('Code Injection')	30-Jul-20	7.2	A potential security vulnerability has been identified in HPE Intelligent Provisioning, Service Pack for ProLiant, and HPE Scripting ToolKit. The vulnerability could be	N/A	H-HPE-SYNE-190820/1342

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			locally exploited to allow arbitrary code execution during the boot process. **Note:** This vulnerability is related to using insmod in GRUB2 in the specific impacted HPE product and HPE is addressing this issue. HPE has made the following software updates and mitigation information to resolve the vulnerability in Intelligent Provisioning, Service Pack for ProLiant, and HPE Scripting ToolKit. HPE provided latest Intelligent Provisioning, Service Pack for ProLiant, and HPE Scripting Toolkit which includes the GRUB2 patch to resolve this vulnerability. These new boot images will update GRUB2 and the Forbidden Signature Database (DBX). After the DBX is updated, users will not be able to boot to the older IP, SPP or Scripting ToolKit with Secure Boot enabled. HPE have provided a standalone DBX update tool to work with Microsoft Windows, and supported Linux Operating Systems. These tools can be used to update the Forbidden Signature Database (DBX) from within the OS. **Note:**		

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			This DBX update mitigates the GRUB2 issue with insmod enabled, and the "Boot Hole" issue for HPE signed GRUB2 applications. **CVE ID : CVE-2020-7205**		
proliant_bl460c_gen8_blade_server					
Improper Control of Generation of Code ('Code Injection')	30-Jul-20	7.2	A potential security vulnerability has been identified in HPE Intelligent Provisioning, Service Pack for ProLiant, and HPE Scripting ToolKit. The vulnerability could be locally exploited to allow arbitrary code execution during the boot process. **Note:** This vulnerability is related to using insmod in GRUB2 in the specific impacted HPE product and HPE is addressing this issue. HPE has made the following software updates and mitigation information to resolve the vulnerability in Intelligent Provisioning, Service Pack for ProLiant, and HPE Scripting ToolKit. HPE provided latest Intelligent Provisioning, Service Pack for ProLiant, and HPE Scripting Toolkit which includes the GRUB2 patch to resolve this vulnerability. These new boot images will update GRUB2 and the Forbidden	N/A	H-HPE-PROL-190820/1343

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Signature Database (DBX). After the DBX is updated, users will not be able to boot to the older IP, SPP or Scripting ToolKit with Secure Boot enabled. HPE have provided a standalone DBX update tool to work with Microsoft Windows, and supported Linux Operating Systems. These tools can be used to update the Forbidden Signature Database (DBX) from within the OS. **Note:** This DBX update mitigates the GRUB2 issue with insmod enabled, and the "Boot Hole" issue for HPE signed GRUB2 applications. **CVE ID : CVE-2020-7205**		
proliant_bl660c_gen8_blade_server					
Improper Control of Generation of Code ('Code Injection')	30-Jul-20	7.2	A potential security vulnerability has been identified in HPE Intelligent Provisioning, Service Pack for ProLiant, and HPE Scripting ToolKit. The vulnerability could be locally exploited to allow arbitrary code execution during the boot process. **Note:** This vulnerability is related to using insmod in GRUB2 in the specific impacted HPE product and HPE is addressing this issue. HPE	N/A	H-HPE-PROL-190820/1344

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			has made the following software updates and mitigation information to resolve the vulnerability in Intelligent Provisioning, Service Pack for ProLiant, and HPE Scripting ToolKit. HPE provided latest Intelligent Provisioning, Service Pack for ProLiant, and HPE Scripting Toolkit which includes the GRUB2 patch to resolve this vulnerability. These new boot images will update GRUB2 and the Forbidden Signature Database (DBX). After the DBX is updated, users will not be able to boot to the older IP, SPP or Scripting ToolKit with Secure Boot enabled. HPE have provided a standalone DBX update tool to work with Microsoft Windows, and supported Linux Operating Systems. These tools can be used to update the Forbidden Signature Database (DBX) from within the OS. **Note:** This DBX update mitigates the GRUB2 issue with insmod enabled, and the "Boot Hole" issue for HPE signed GRUB2 applications. **CVE ID : CVE-2020-7205**		
proliant_dl160_gen8_server					

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Improper Control of Generation of Code ('Code Injection')	30-Jul-20	7.2	A potential security vulnerability has been identified in HPE Intelligent Provisioning, Service Pack for ProLiant, and HPE Scripting ToolKit. The vulnerability could be locally exploited to allow arbitrary code execution during the boot process. **Note:** This vulnerability is related to using insmod in GRUB2 in the specific impacted HPE product and HPE is addressing this issue. HPE has made the following software updates and mitigation information to resolve the vulnerability in Intelligent Provisioning, Service Pack for ProLiant, and HPE Scripting ToolKit. HPE provided latest Intelligent Provisioning, Service Pack for ProLiant, and HPE Scripting Toolkit which includes the GRUB2 patch to resolve this vulnerability. These new boot images will update GRUB2 and the Forbidden Signature Database (DBX). After the DBX is updated, users will not be able to boot to the older IP, SPP or Scripting ToolKit with Secure Boot enabled. HPE have provided a standalone DBX update tool to work with	N/A	H-HPE-PROL-190820/1345

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Microsoft Windows, and supported Linux Operating Systems. These tools can be used to update the Forbidden Signature Database (DBX) from within the OS. **Note:** This DBX update mitigates the GRUB2 issue with insmod enabled, and the "Boot Hole" issue for HPE signed GRUB2 applications. **CVE ID : CVE-2020-7205**		
proliant_dl360e_gen8_server					
Improper Control of Generation of Code ('Code Injection')	30-Jul-20	7.2	A potential security vulnerability has been identified in HPE Intelligent Provisioning, Service Pack for ProLiant, and HPE Scripting ToolKit. The vulnerability could be locally exploited to allow arbitrary code execution during the boot process. **Note:** This vulnerability is related to using insmod in GRUB2 in the specific impacted HPE product and HPE is addressing this issue. HPE has made the following software updates and mitigation information to resolve the vulnerability in Intelligent Provisioning, Service Pack for ProLiant, and HPE Scripting ToolKit. HPE provided latest Intelligent Provisioning,	N/A	H-HPE-PROL-190820/1346

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Service Pack for ProLiant, and HPE Scripting Toolkit which includes the GRUB2 patch to resolve this vulnerability. These new boot images will update GRUB2 and the Forbidden Signature Database (DBX). After the DBX is updated, users will not be able to boot to the older IP, SPP or Scripting ToolKit with Secure Boot enabled. HPE have provided a standalone DBX update tool to work with Microsoft Windows, and supported Linux Operating Systems. These tools can be used to update the Forbidden Signature Database (DBX) from within the OS. **Note:** This DBX update mitigates the GRUB2 issue with insmod enabled, and the "Boot Hole" issue for HPE signed GRUB2 applications. **CVE ID : CVE-2020-7205**		
proliant_dl360p_gen8_server					
Improper Control of Generation of Code ('Code Injection')	30-Jul-20	7.2	A potential security vulnerability has been identified in HPE Intelligent Provisioning, Service Pack for ProLiant, and HPE Scripting ToolKit. The vulnerability could be locally exploited to allow arbitrary code execution	N/A	H-HPE-PROL-190820/1347

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			during the boot process. **Note:** This vulnerability is related to using insmod in GRUB2 in the specific impacted HPE product and HPE is addressing this issue. HPE has made the following software updates and mitigation information to resolve the vulnerability in Intelligent Provisioning, Service Pack for ProLiant, and HPE Scripting ToolKit. HPE provided latest Intelligent Provisioning, Service Pack for ProLiant, and HPE Scripting Toolkit which includes the GRUB2 patch to resolve this vulnerability. These new boot images will update GRUB2 and the Forbidden Signature Database (DBX). After the DBX is updated, users will not be able to boot to the older IP, SPP or Scripting ToolKit with Secure Boot enabled. HPE have provided a standalone DBX update tool to work with Microsoft Windows, and supported Linux Operating Systems. These tools can be used to update the Forbidden Signature Database (DBX) from within the OS. **Note:** This DBX update mitigates the GRUB2 issue with		

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			insmod enabled, and the "Boot Hole" issue for HPE signed GRUB2 applications. **CVE ID : CVE-2020-7205**		
proliant_dl380e_gen8_server					
Improper Control of Generation of Code ('Code Injection')	30-Jul-20	7.2	A potential security vulnerability has been identified in HPE Intelligent Provisioning, Service Pack for ProLiant, and HPE Scripting ToolKit. The vulnerability could be locally exploited to allow arbitrary code execution during the boot process. **Note:** This vulnerability is related to using insmod in GRUB2 in the specific impacted HPE product and HPE is addressing this issue. HPE has made the following software updates and mitigation information to resolve the vulnerability in Intelligent Provisioning, Service Pack for ProLiant, and HPE Scripting ToolKit. HPE provided latest Intelligent Provisioning, Service Pack for ProLiant, and HPE Scripting Toolkit which includes the GRUB2 patch to resolve this vulnerability. These new boot images will update GRUB2 and the Forbidden Signature Database (DBX). After the DBX is updated,	N/A	H-HPE-PROL-190820/1348

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			users will not be able to boot to the older IP, SPP or Scripting ToolKit with Secure Boot enabled. HPE have provided a standalone DBX update tool to work with Microsoft Windows, and supported Linux Operating Systems. These tools can be used to update the Forbidden Signature Database (DBX) from within the OS. **Note:** This DBX update mitigates the GRUB2 issue with insmod enabled, and the "Boot Hole" issue for HPE signed GRUB2 applications. **CVE ID : CVE-2020-7205**		
proliant_dl380p_gen8_server					
Improper Control of Generation of Code ('Code Injection')	30-Jul-20	7.2	A potential security vulnerability has been identified in HPE Intelligent Provisioning, Service Pack for ProLiant, and HPE Scripting ToolKit. The vulnerability could be locally exploited to allow arbitrary code execution during the boot process. **Note:** This vulnerability is related to using insmod in GRUB2 in the specific impacted HPE product and HPE is addressing this issue. HPE has made the following software updates and	N/A	H-HPE-PROL-190820/1349

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			mitigation information to resolve the vulnerability in Intelligent Provisioning, Service Pack for ProLiant, and HPE Scripting ToolKit. HPE provided latest Intelligent Provisioning, Service Pack for ProLiant, and HPE Scripting Toolkit which includes the GRUB2 patch to resolve this vulnerability. These new boot images will update GRUB2 and the Forbidden Signature Database (DBX). After the DBX is updated, users will not be able to boot to the older IP, SPP or Scripting ToolKit with Secure Boot enabled. HPE have provided a standalone DBX update tool to work with Microsoft Windows, and supported Linux Operating Systems. These tools can be used to update the Forbidden Signature Database (DBX) from within the OS. **Note:** This DBX update mitigates the GRUB2 issue with insmod enabled, and the "Boot Hole" issue for HPE signed GRUB2 applications. **CVE ID : CVE-2020-7205**		
proliant_dl385p_gen8_server					
Improper Control of	30-Jul-20	7.2	A potential security vulnerability has been	N/A	H-HPE-PROL-190820/1350

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Generation of Code ('Code Injection')			identified in HPE Intelligent Provisioning, Service Pack for ProLiant, and HPE Scripting ToolKit. The vulnerability could be locally exploited to allow arbitrary code execution during the boot process. **Note:** This vulnerability is related to using insmod in GRUB2 in the specific impacted HPE product and HPE is addressing this issue. HPE has made the following software updates and mitigation information to resolve the vulnerability in Intelligent Provisioning, Service Pack for ProLiant, and HPE Scripting ToolKit. HPE provided latest Intelligent Provisioning, Service Pack for ProLiant, and HPE Scripting Toolkit which includes the GRUB2 patch to resolve this vulnerability. These new boot images will update GRUB2 and the Forbidden Signature Database (DBX). After the DBX is updated, users will not be able to boot to the older IP, SPP or Scripting ToolKit with Secure Boot enabled. HPE have provided a standalone DBX update tool to work with Microsoft Windows, and supported Linux Operating		

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Systems. These tools can be used to update the Forbidden Signature Database (DBX) from within the OS. **Note:** This DBX update mitigates the GRUB2 issue with insmod enabled, and the "Boot Hole" issue for HPE signed GRUB2 applications. **CVE ID : CVE-2020-7205**		
proliant_dl560_gen8_server					
Improper Control of Generation of Code ('Code Injection')	30-Jul-20	7.2	A potential security vulnerability has been identified in HPE Intelligent Provisioning, Service Pack for ProLiant, and HPE Scripting ToolKit. The vulnerability could be locally exploited to allow arbitrary code execution during the boot process. **Note:** This vulnerability is related to using insmod in GRUB2 in the specific impacted HPE product and HPE is addressing this issue. HPE has made the following software updates and mitigation information to resolve the vulnerability in Intelligent Provisioning, Service Pack for ProLiant, and HPE Scripting ToolKit. HPE provided latest Intelligent Provisioning, Service Pack for ProLiant, and HPE Scripting Toolkit	N/A	H-HPE-PROL-190820/1351

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			which includes the GRUB2 patch to resolve this vulnerability. These new boot images will update GRUB2 and the Forbidden Signature Database (DBX). After the DBX is updated, users will not be able to boot to the older IP, SPP or Scripting ToolKit with Secure Boot enabled. HPE have provided a standalone DBX update tool to work with Microsoft Windows, and supported Linux Operating Systems. These tools can be used to update the Forbidden Signature Database (DBX) from within the OS. **Note:** This DBX update mitigates the GRUB2 issue with insmod enabled, and the "Boot Hole" issue for HPE signed GRUB2 applications. **CVE ID : CVE-2020-7205**		
proliant_dl580_gen8_server					
Improper Control of Generation of Code ('Code Injection')	30-Jul-20	7.2	A potential security vulnerability has been identified in HPE Intelligent Provisioning, Service Pack for ProLiant, and HPE Scripting ToolKit. The vulnerability could be locally exploited to allow arbitrary code execution during the boot process. **Note:** This	N/A	H-HPE-PROL-190820/1352

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			vulnerability is related to using insmod in GRUB2 in the specific impacted HPE product and HPE is addressing this issue. HPE has made the following software updates and mitigation information to resolve the vulnerability in Intelligent Provisioning, Service Pack for ProLiant, and HPE Scripting ToolKit. HPE provided latest Intelligent Provisioning, Service Pack for ProLiant, and HPE Scripting Toolkit which includes the GRUB2 patch to resolve this vulnerability. These new boot images will update GRUB2 and the Forbidden Signature Database (DBX). After the DBX is updated, users will not be able to boot to the older IP, SPP or Scripting ToolKit with Secure Boot enabled. HPE have provided a standalone DBX update tool to work with Microsoft Windows, and supported Linux Operating Systems. These tools can be used to update the Forbidden Signature Database (DBX) from within the OS. **Note:** This DBX update mitigates the GRUB2 issue with insmod enabled, and the "Boot Hole" issue for HPE		

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			signed GRUB2 applications. **CVE ID : CVE-2020-7205**		
proliant_ml310e_gen8_server					
Improper Control of Generation of Code ('Code Injection')	30-Jul-20	7.2	A potential security vulnerability has been identified in HPE Intelligent Provisioning, Service Pack for ProLiant, and HPE Scripting ToolKit. The vulnerability could be locally exploited to allow arbitrary code execution during the boot process. **Note:** This vulnerability is related to using insmod in GRUB2 in the specific impacted HPE product and HPE is addressing this issue. HPE has made the following software updates and mitigation information to resolve the vulnerability in Intelligent Provisioning, Service Pack for ProLiant, and HPE Scripting ToolKit. HPE provided latest Intelligent Provisioning, Service Pack for ProLiant, and HPE Scripting Toolkit which includes the GRUB2 patch to resolve this vulnerability. These new boot images will update GRUB2 and the Forbidden Signature Database (DBX). After the DBX is updated, users will not be able to boot to the older IP, SPP or	N/A	H-HPE-PROL-190820/1353

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Scripting ToolKit with Secure Boot enabled. HPE have provided a standalone DBX update tool to work with Microsoft Windows, and supported Linux Operating Systems. These tools can be used to update the Forbidden Signature Database (DBX) from within the OS. **Note:** This DBX update mitigates the GRUB2 issue with insmod enabled, and the "Boot Hole" issue for HPE signed GRUB2 applications. **CVE ID : CVE-2020-7205**		
proliant_ml350e_gen8_server					
Improper Control of Generation of Code ('Code Injection')	30-Jul-20	7.2	A potential security vulnerability has been identified in HPE Intelligent Provisioning, Service Pack for ProLiant, and HPE Scripting ToolKit. The vulnerability could be locally exploited to allow arbitrary code execution during the boot process. **Note:** This vulnerability is related to using insmod in GRUB2 in the specific impacted HPE product and HPE is addressing this issue. HPE has made the following software updates and mitigation information to resolve the vulnerability in	N/A	H-HPE-PROL-190820/1354

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Intelligent Provisioning, Service Pack for ProLiant, and HPE Scripting ToolKit. HPE provided latest Intelligent Provisioning, Service Pack for ProLiant, and HPE Scripting Toolkit which includes the GRUB2 patch to resolve this vulnerability. These new boot images will update GRUB2 and the Forbidden Signature Database (DBX). After the DBX is updated, users will not be able to boot to the older IP, SPP or Scripting ToolKit with Secure Boot enabled. HPE have provided a standalone DBX update tool to work with Microsoft Windows, and supported Linux Operating Systems. These tools can be used to update the Forbidden Signature Database (DBX) from within the OS. **Note:** This DBX update mitigates the GRUB2 issue with insmod enabled, and the "Boot Hole" issue for HPE signed GRUB2 applications. **CVE ID : CVE-2020-7205**		
proliant_ml350p_gen8_server					
Improper Control of Generation of Code	30-Jul-20	7.2	A potential security vulnerability has been identified in HPE Intelligent Provisioning,	N/A	H-HPE-PROL-190820/1355

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
('Code Injection')			Service Pack for ProLiant, and HPE Scripting ToolKit. The vulnerability could be locally exploited to allow arbitrary code execution during the boot process. **Note:** This vulnerability is related to using insmod in GRUB2 in the specific impacted HPE product and HPE is addressing this issue. HPE has made the following software updates and mitigation information to resolve the vulnerability in Intelligent Provisioning, Service Pack for ProLiant, and HPE Scripting ToolKit. HPE provided latest Intelligent Provisioning, Service Pack for ProLiant, and HPE Scripting Toolkit which includes the GRUB2 patch to resolve this vulnerability. These new boot images will update GRUB2 and the Forbidden Signature Database (DBX). After the DBX is updated, users will not be able to boot to the older IP, SPP or Scripting ToolKit with Secure Boot enabled. HPE have provided a standalone DBX update tool to work with Microsoft Windows, and supported Linux Operating Systems. These tools can be used to update the		

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Forbidden Signature Database (DBX) from within the OS. **Note:** This DBX update mitigates the GRUB2 issue with insmod enabled, and the "Boot Hole" issue for HPE signed GRUB2 applications. **CVE ID : CVE-2020-7205**		
proliant_sl230s_gen8_server					
Improper Control of Generation of Code ('Code Injection')	30-Jul-20	7.2	A potential security vulnerability has been identified in HPE Intelligent Provisioning, Service Pack for ProLiant, and HPE Scripting ToolKit. The vulnerability could be locally exploited to allow arbitrary code execution during the boot process. **Note:** This vulnerability is related to using insmod in GRUB2 in the specific impacted HPE product and HPE is addressing this issue. HPE has made the following software updates and mitigation information to resolve the vulnerability in Intelligent Provisioning, Service Pack for ProLiant, and HPE Scripting ToolKit. HPE provided latest Intelligent Provisioning, Service Pack for ProLiant, and HPE Scripting Toolkit which includes the GRUB2 patch to resolve this	N/A	H-HPE-PROL-190820/1356

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			vulnerability. These new boot images will update GRUB2 and the Forbidden Signature Database (DBX). After the DBX is updated, users will not be able to boot to the older IP, SPP or Scripting ToolKit with Secure Boot enabled. HPE have provided a standalone DBX update tool to work with Microsoft Windows, and supported Linux Operating Systems. These tools can be used to update the Forbidden Signature Database (DBX) from within the OS. **Note:** This DBX update mitigates the GRUB2 issue with insmod enabled, and the "Boot Hole" issue for HPE signed GRUB2 applications. **CVE ID : CVE-2020-7205**		
proliant_sl250s_gen8_server					
Improper Control of Generation of Code ('Code Injection')	30-Jul-20	7.2	A potential security vulnerability has been identified in HPE Intelligent Provisioning, Service Pack for ProLiant, and HPE Scripting ToolKit. The vulnerability could be locally exploited to allow arbitrary code execution during the boot process. **Note:** This vulnerability is related to using insmod in GRUB2 in	N/A	H-HPE-PROL-190820/1357

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			the specific impacted HPE product and HPE is addressing this issue. HPE has made the following software updates and mitigation information to resolve the vulnerability in Intelligent Provisioning, Service Pack for ProLiant, and HPE Scripting ToolKit. HPE provided latest Intelligent Provisioning, Service Pack for ProLiant, and HPE Scripting Toolkit which includes the GRUB2 patch to resolve this vulnerability. These new boot images will update GRUB2 and the Forbidden Signature Database (DBX). After the DBX is updated, users will not be able to boot to the older IP, SPP or Scripting ToolKit with Secure Boot enabled. HPE have provided a standalone DBX update tool to work with Microsoft Windows, and supported Linux Operating Systems. These tools can be used to update the Forbidden Signature Database (DBX) from within the OS. **Note:** This DBX update mitigates the GRUB2 issue with insmod enabled, and the "Boot Hole" issue for HPE signed GRUB2 applications.		

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2020-7205		
proliant_sl270s_gen8_server					
Improper Control of Generation of Code ('Code Injection')	30-Jul-20	7.2	A potential security vulnerability has been identified in HPE Intelligent Provisioning, Service Pack for ProLiant, and HPE Scripting ToolKit. The vulnerability could be locally exploited to allow arbitrary code execution during the boot process. **Note:** This vulnerability is related to using insmod in GRUB2 in the specific impacted HPE product and HPE is addressing this issue. HPE has made the following software updates and mitigation information to resolve the vulnerability in Intelligent Provisioning, Service Pack for ProLiant, and HPE Scripting ToolKit. HPE provided latest Intelligent Provisioning, Service Pack for ProLiant, and HPE Scripting Toolkit which includes the GRUB2 patch to resolve this vulnerability. These new boot images will update GRUB2 and the Forbidden Signature Database (DBX). After the DBX is updated, users will not be able to boot to the older IP, SPP or Scripting ToolKit with Secure Boot enabled. HPE have provided a	N/A	H-HPE-PROL-190820/1358

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			standalone DBX update tool to work with Microsoft Windows, and supported Linux Operating Systems. These tools can be used to update the Forbidden Signature Database (DBX) from within the OS. **Note:** This DBX update mitigates the GRUB2 issue with insmod enabled, and the "Boot Hole" issue for HPE signed GRUB2 applications. **CVE ID : CVE-2020-7205**		
proliant_sl4540_gen8_server					
Improper Control of Generation of Code ('Code Injection')	30-Jul-20	7.2	A potential security vulnerability has been identified in HPE Intelligent Provisioning, Service Pack for ProLiant, and HPE Scripting ToolKit. The vulnerability could be locally exploited to allow arbitrary code execution during the boot process. **Note:** This vulnerability is related to using insmod in GRUB2 in the specific impacted HPE product and HPE is addressing this issue. HPE has made the following software updates and mitigation information to resolve the vulnerability in Intelligent Provisioning, Service Pack for ProLiant, and HPE Scripting ToolKit.	N/A	H-HPE-PROL-190820/1359

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			HPE provided latest Intelligent Provisioning, Service Pack for ProLiant, and HPE Scripting Toolkit which includes the GRUB2 patch to resolve this vulnerability. These new boot images will update GRUB2 and the Forbidden Signature Database (DBX). After the DBX is updated, users will not be able to boot to the older IP, SPP or Scripting ToolKit with Secure Boot enabled. HPE have provided a standalone DBX update tool to work with Microsoft Windows, and supported Linux Operating Systems. These tools can be used to update the Forbidden Signature Database (DBX) from within the OS. **Note:** This DBX update mitigates the GRUB2 issue with insmod enabled, and the "Boot Hole" issue for HPE signed GRUB2 applications. **CVE ID : CVE-2020-7205**		
proliant_ws460c_gen8_graphics_server_blade					
Improper Control of Generation of Code ('Code Injection')	30-Jul-20	7.2	A potential security vulnerability has been identified in HPE Intelligent Provisioning, Service Pack for ProLiant, and HPE Scripting ToolKit. The vulnerability could be	N/A	H-HPE-PROL-190820/1360

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			locally exploited to allow arbitrary code execution during the boot process. **Note:** This vulnerability is related to using insmod in GRUB2 in the specific impacted HPE product and HPE is addressing this issue. HPE has made the following software updates and mitigation information to resolve the vulnerability in Intelligent Provisioning, Service Pack for ProLiant, and HPE Scripting ToolKit. HPE provided latest Intelligent Provisioning, Service Pack for ProLiant, and HPE Scripting Toolkit which includes the GRUB2 patch to resolve this vulnerability. These new boot images will update GRUB2 and the Forbidden Signature Database (DBX). After the DBX is updated, users will not be able to boot to the older IP, SPP or Scripting ToolKit with Secure Boot enabled. HPE have provided a standalone DBX update tool to work with Microsoft Windows, and supported Linux Operating Systems. These tools can be used to update the Forbidden Signature Database (DBX) from within the OS. **Note:**		

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			This DBX update mitigates the GRUB2 issue with insmod enabled, and the "Boot Hole" issue for HPE signed GRUB2 applications. **CVE ID : CVE-2020-7205**		
apollo_4520_chassis					
Improper Control of Generation of Code ('Code Injection')	30-Jul-20	7.2	A potential security vulnerability has been identified in HPE Intelligent Provisioning, Service Pack for ProLiant, and HPE Scripting ToolKit. The vulnerability could be locally exploited to allow arbitrary code execution during the boot process. **Note:** This vulnerability is related to using insmod in GRUB2 in the specific impacted HPE product and HPE is addressing this issue. HPE has made the following software updates and mitigation information to resolve the vulnerability in Intelligent Provisioning, Service Pack for ProLiant, and HPE Scripting ToolKit. HPE provided latest Intelligent Provisioning, Service Pack for ProLiant, and HPE Scripting Toolkit which includes the GRUB2 patch to resolve this vulnerability. These new boot images will update GRUB2 and the Forbidden	N/A	H-HPE-APOL-190820/1361

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Signature Database (DBX). After the DBX is updated, users will not be able to boot to the older IP, SPP or Scripting ToolKit with Secure Boot enabled. HPE have provided a standalone DBX update tool to work with Microsoft Windows, and supported Linux Operating Systems. These tools can be used to update the Forbidden Signature Database (DBX) from within the OS. **Note:** This DBX update mitigates the GRUB2 issue with insmod enabled, and the "Boot Hole" issue for HPE signed GRUB2 applications. **CVE ID : CVE-2020-7205**		
cloudline_cl3100_gen9_server					
Improper Control of Generation of Code ('Code Injection')	30-Jul-20	7.2	A potential security vulnerability has been identified in HPE Intelligent Provisioning, Service Pack for ProLiant, and HPE Scripting ToolKit. The vulnerability could be locally exploited to allow arbitrary code execution during the boot process. **Note:** This vulnerability is related to using insmod in GRUB2 in the specific impacted HPE product and HPE is addressing this issue. HPE	N/A	H-HPE-CLOU-190820/1362

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			has made the following software updates and mitigation information to resolve the vulnerability in Intelligent Provisioning, Service Pack for ProLiant, and HPE Scripting ToolKit. HPE provided latest Intelligent Provisioning, Service Pack for ProLiant, and HPE Scripting Toolkit which includes the GRUB2 patch to resolve this vulnerability. These new boot images will update GRUB2 and the Forbidden Signature Database (DBX). After the DBX is updated, users will not be able to boot to the older IP, SPP or Scripting ToolKit with Secure Boot enabled. HPE have provided a standalone DBX update tool to work with Microsoft Windows, and supported Linux Operating Systems. These tools can be used to update the Forbidden Signature Database (DBX) from within the OS. **Note:** This DBX update mitigates the GRUB2 issue with insmod enabled, and the "Boot Hole" issue for HPE signed GRUB2 applications. **CVE ID : CVE-2020-7205**		
cloudline_cl5200_gen9_server					

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Improper Control of Generation of Code ('Code Injection')	30-Jul-20	7.2	A potential security vulnerability has been identified in HPE Intelligent Provisioning, Service Pack for ProLiant, and HPE Scripting ToolKit. The vulnerability could be locally exploited to allow arbitrary code execution during the boot process. **Note:** This vulnerability is related to using insmod in GRUB2 in the specific impacted HPE product and HPE is addressing this issue. HPE has made the following software updates and mitigation information to resolve the vulnerability in Intelligent Provisioning, Service Pack for ProLiant, and HPE Scripting ToolKit. HPE provided latest Intelligent Provisioning, Service Pack for ProLiant, and HPE Scripting Toolkit which includes the GRUB2 patch to resolve this vulnerability. These new boot images will update GRUB2 and the Forbidden Signature Database (DBX). After the DBX is updated, users will not be able to boot to the older IP, SPP or Scripting ToolKit with Secure Boot enabled. HPE have provided a standalone DBX update tool to work with	N/A	H-HPE-CLOU-190820/1363

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Microsoft Windows, and supported Linux Operating Systems. These tools can be used to update the Forbidden Signature Database (DBX) from within the OS. **Note:** This DBX update mitigates the GRUB2 issue with insmod enabled, and the "Boot Hole" issue for HPE signed GRUB2 applications. **CVE ID : CVE-2020-7205**		
cloudline_cl5800_gen9_server					
Improper Control of Generation of Code ('Code Injection')	30-Jul-20	7.2	A potential security vulnerability has been identified in HPE Intelligent Provisioning, Service Pack for ProLiant, and HPE Scripting ToolKit. The vulnerability could be locally exploited to allow arbitrary code execution during the boot process. **Note:** This vulnerability is related to using insmod in GRUB2 in the specific impacted HPE product and HPE is addressing this issue. HPE has made the following software updates and mitigation information to resolve the vulnerability in Intelligent Provisioning, Service Pack for ProLiant, and HPE Scripting ToolKit. HPE provided latest Intelligent Provisioning,	N/A	H-HPE-CLOU-190820/1364

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Service Pack for ProLiant, and HPE Scripting Toolkit which includes the GRUB2 patch to resolve this vulnerability. These new boot images will update GRUB2 and the Forbidden Signature Database (DBX). After the DBX is updated, users will not be able to boot to the older IP, SPP or Scripting ToolKit with Secure Boot enabled. HPE have provided a standalone DBX update tool to work with Microsoft Windows, and supported Linux Operating Systems. These tools can be used to update the Forbidden Signature Database (DBX) from within the OS. **Note:** This DBX update mitigates the GRUB2 issue with insmod enabled, and the "Boot Hole" issue for HPE signed GRUB2 applications. **CVE ID : CVE-2020-7205**		
Huawei					
cloudengine_6800					
Information Exposure	17-Jul-20	2.1	There is a information leak vulnerability in some Huawei products, and it could allow a local attacker to get information. The vulnerability is due to the improper management of the username. An attacker	https://www.huawei.com/en/psirt/security-advisories/huawei-sa-20200715-03-	H-HUA-CLOU-190820/1365

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			with the ability to access the device and cause the username information leak. Affected product versions include: CloudEngine 12800 versions V200R002C50SPC800, V200R003C00SPC810, V200R005C00SPC800, V200R005C10SPC800, V200R019C00SPC800; CloudEngine 5800 versions V200R002C50SPC800, V200R003C00SPC810, V200R005C00SPC800, V200R005C10SPC800, V200R019C00SPC800; CloudEngine 6800 versions V200R002C50SPC800, V200R003C00SPC810, V200R005C00SPC800, V200R005C10SPC800, V200R005C20SPC800, V200R019C00SPC800; CloudEngine 7800 versions V200R002C50SPC800, V200R003C00SPC810, V200R005C00SPC800, V200R005C10SPC800, V200R019C00SPC800 **CVE ID : CVE-2020-9102**	informationleak-en	
mate_30_pro					
N/A	18-Jul-20	4.3	Huawei Mate 30 Pro smartphones with versions earlier than 10.1.0.150(C00E136R5P3)	https://www.huawei.com/en/psirt/security-	H-HUA-MATE-190820/1366

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			have an improper authorization vulnerability. The system does not properly restrict the use of system service by applications, the attacker should trick the user into installing a malicious application, successful exploit could cause a denial of audio service. **CVE ID : CVE-2020-9256**	advisories/huawei-sa-20200715-05-smartphone-en	
cloudengine_5800					
Information Exposure	17-Jul-20	2.1	There is a information leak vulnerability in some Huawei products, and it could allow a local attacker to get information. The vulnerability is due to the improper management of the username. An attacker with the ability to access the device and cause the username information leak. Affected product versions include: CloudEngine 12800 versions V200R002C50SPC800, V200R003C00SPC810, V200R005C00SPC800, V200R005C10SPC800, V200R019C00SPC800; CloudEngine 5800 versions V200R002C50SPC800, V200R003C00SPC810, V200R005C00SPC800, V200R005C10SPC800,	https://www.huawei.com/en/psirt/security-advisories/huawei-sa-20200715-03-informationleak-en	H-HUA-CLOU-190820/1367

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			V200R019C00SPC800; CloudEngine 6800 versions V200R002C50SPC800, V200R003C00SPC810, V200R005C00SPC800, V200R005C10SPC800, V200R005C20SPC800, V200R019C00SPC800; CloudEngine 7800 versions V200R002C50SPC800, V200R003C00SPC810, V200R005C00SPC800, V200R005C10SPC800, V200R019C00SPC800 **CVE ID : CVE-2020-9102**		
cloudengine_7800					
Information Exposure	17-Jul-20	2.1	There is a information leak vulnerability in some Huawei products, and it could allow a local attacker to get information. The vulnerability is due to the improper management of the username. An attacker with the ability to access the device and cause the username information leak. Affected product versions include: CloudEngine 12800 versions V200R002C50SPC800, V200R003C00SPC810, V200R005C00SPC800, V200R005C10SPC800, V200R019C00SPC800; CloudEngine 5800 versions	https://www.huawei.com/en/psirt/security-advisories/huawei-sa-20200715-03-informationleak-en	H-HUA-CLOU-190820/1368

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			V200R002C50SPC800, V200R003C00SPC810, V200R005C00SPC800, V200R005C10SPC800, V200R019C00SPC800; CloudEngine 6800 versions V200R002C50SPC800, V200R003C00SPC810, V200R005C00SPC800, V200R005C10SPC800, V200R005C20SPC800, V200R019C00SPC800; CloudEngine 7800 versions V200R002C50SPC800, V200R003C00SPC810, V200R005C00SPC800, V200R005C10SPC800, V200R019C00SPC800 **CVE ID : CVE-2020-9102**		
moana-al00b					
Missing Initialization of Resource	17-Jul-20	4.3	Huawei Smart Phones Moana-AL00B with versions earlier than 10.1.0.166 have a missing initialization of resource vulnerability. An attacker tricks the user into installing then running a crafted application. Due to improper initialization of specific parameters, successful exploit of this vulnerability may cause device exceptions. **CVE ID : CVE-2020-9227**	https://www.huawei.com/en/psirt/security-advisories/huawei-sa-20200715-09-smartphone-en	H-HUA-MOAN-190820/1369
magic2					
Improper	17-Jul-20	2.1	HUAWEI Mate 20 versions	https://ww	H-HUA-MAGI-

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Limitation of a Pathname to a Restricted Directory ('Path Traversal')			earlier than 10.1.0.160(C00E160R3P8), HUAWEI Mate 20 X versions earlier than 10.1.0.135(C00E135R2P8), HUAWEI Mate 20 RS versions earlier than 10.1.0.160(C786E160R3P8), and Honor Magic2 smartphones versions earlier than 10.1.0.160(C00E160R2P11) have a path traversal vulnerability. The system does not sufficiently validate certain pathname from certain process, successful exploit could allow the attacker write files to a crafted path. **CVE ID : CVE-2020-9252**	w.huawei.com/en/psirt/security-advisories/huawei-sa-20200715-07-smartphone-en	190820/1370
ips_module					
Out-of-bounds Write	18-Jul-20	3.3	There is an out-of-bounds write vulnerability in some products. An unauthenticated attacker crafts malformed packets with specific parameter and sends the packets to the affected products. Due to insufficient validation of packets, which may be exploited to cause the process reboot. Affected product versions include: IPS Module versions V500R005C00, V500R005C10; NGFW Module versions V500R005C00,	https://www.huawei.com/en/psirt/security-advisories/huawei-sa-20200715-01-outofbounds write-en	H-HUA-IPS_-190820/1371

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			V500R005C10; Secospace USG6300 versions V500R001C30, V500R001C60, V500R005C00, V500R005C10; Secospace USG6500 versions V500R001C30, V500R001C60, V500R005C00, V500R005C10; Secospace USG6600 versions V500R001C30, V500R001C60, V500R005C00, V500R005C10; USG9500 versions V500R001C30, V500R001C60, V500R005C00, V500R005C10 **CVE ID : CVE-2020-9101**		
cloudengine_12800					
Information Exposure	17-Jul-20	2.1	There is a information leak vulnerability in some Huawei products, and it could allow a local attacker to get information. The vulnerability is due to the improper management of the username. An attacker with the ability to access the device and cause the username information leak. Affected product versions include: CloudEngine 12800 versions V200R002C50SPC800, V200R003C00SPC810, V200R005C00SPC800,	https://www.huawei.com/en/psirt/security-advisories/huawei-sa-20200715-03-informationleak-en	H-HUA-CLOU-190820/1372

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			V200R005C10SPC800, V200R019C00SPC800; CloudEngine 5800 versions V200R002C50SPC800, V200R003C00SPC810, V200R005C00SPC800, V200R005C10SPC800, V200R019C00SPC800; CloudEngine 6800 versions V200R002C50SPC800, V200R003C00SPC810, V200R005C00SPC800, V200R005C10SPC800, V200R005C20SPC800, V200R019C00SPC800; CloudEngine 7800 versions V200R002C50SPC800, V200R003C00SPC810, V200R005C00SPC800, V200R005C10SPC800, V200R019C00SPC800 **CVE ID : CVE-2020-9102**		
honor_v30					
Improper Authentication	17-Jul-20	4.3	Huawei Honor V30 smartphones with versions earlier than 10.1.0.212(C00E210R5P1) have an improper authentication vulnerability. The system does not sufficiently validate certain parameter passed from the bottom level, the attacker should trick the user into installing a malicious application and control the	https://www.huawei.com/en/psirt/security-advisories/huawei-sa-20200715-02-smartphone-en	H-HUA-HONO-190820/1373

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			bottom level, successful exploit could cause information disclosure. **CVE ID : CVE-2020-9259**		
secospace_usg6300					
Out-of-bounds Write	18-Jul-20	3.3	There is an out-of-bounds write vulnerability in some products. An unauthenticated attacker crafts malformed packets with specific parameter and sends the packets to the affected products. Due to insufficient validation of packets, which may be exploited to cause the process reboot. Affected product versions include: IPS Module versions V500R005C00, V500R005C10; NGFW Module versions V500R005C00, V500R005C10; Secospace USG6300 versions V500R001C30, V500R001C60, V500R005C00, V500R005C10; Secospace USG6500 versions V500R001C30, V500R001C60, V500R005C00, V500R005C10; Secospace USG6600 versions V500R001C30, V500R001C60, V500R005C00, V500R005C10; USG9500 versions V500R001C30,	https://www.huawei.com/en/psirt/security-advisories/huawei-sa-20200715-01-outofboundswrite-en	H-HUA-SECO-190820/1374

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			V500R001C60, V500R005C00, V500R005C10 **CVE ID : CVE-2020-9101**		
secospace_usg6500					
Out-of-bounds Write	18-Jul-20	3.3	There is an out-of-bounds write vulnerability in some products. An unauthenticated attacker crafts malformed packets with specific parameter and sends the packets to the affected products. Due to insufficient validation of packets, which may be exploited to cause the process reboot. Affected product versions include: IPS Module versions V500R005C00, V500R005C10; NGFW Module versions V500R005C00, V500R005C10; Secospace USG6300 versions V500R001C30, V500R001C60, V500R005C00, V500R005C10; Secospace USG6500 versions V500R001C30, V500R001C60, V500R005C00, V500R005C10; Secospace USG6600 versions V500R001C30, V500R001C60, V500R005C00, V500R005C10; USG9500 versions V500R001C30,	https://www.huawei.com/en/psirt/security-advisories/huawei-sa-20200715-01-outofbounds write-en	H-HUA-SECO-190820/1375

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			V500R001C60, V500R005C00, V500R005C10 **CVE ID : CVE-2020-9101**		
secospace_usg6600					
Out-of-bounds Write	18-Jul-20	3.3	There is an out-of-bounds write vulnerability in some products. An unauthenticated attacker crafts malformed packets with specific parameter and sends the packets to the affected products. Due to insufficient validation of packets, which may be exploited to cause the process reboot. Affected product versions include: IPS Module versions V500R005C00, V500R005C10; NGFW Module versions V500R005C00, V500R005C10; Secospace USG6300 versions V500R001C30, V500R001C60, V500R005C00, V500R005C10; Secospace USG6500 versions V500R001C30, V500R001C60, V500R005C00, V500R005C10; Secospace USG6600 versions V500R001C30, V500R001C60, V500R005C00, V500R005C10; USG9500 versions V500R001C30,	https://www.huawei.com/en/psirt/security-advisories/huawei-sa-20200715-01-outofbounds write-en	H-HUA-SECO-190820/1376

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			V500R001C60, V500R005C00, V500R005C10 **CVE ID : CVE-2020-9101**		
p30_pro					
Improper Neutralization of Special Elements in Output Used by a Downstream Component ('Injection')	17-Jul-20	6.8	HUAWEI P30 Pro smartphones with versions earlier than 10.1.0.123(C432E19R2P5 patch02), versions earlier than 10.1.0.126(C10E11R5P1), and versions earlier than 10.1.0.160(C00E160R2P8) have a logic check error vulnerability. A logic error occurs when the software checking the size of certain parameter, the attacker should trick the user into installing a malicious application, successful exploit may cause code execution. **CVE ID : CVE-2020-9254**	https://www.huawei.com/en/psirt/security-advisories/huawei-sa-20200715-04-smartphone-en	H-HUA-P30_-190820/1377
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	17-Jul-20	6.8	HUAWEI P30 Pro smartphones with versions earlier than 10.1.0.123(C432E19R2P5 patch02), versions earlier than 10.1.0.126(C10E11R5P1), and versions earlier than 10.1.0.160(C00E160R2P8) have a buffer overflow vulnerability. The software access data past the end, or before the beginning, of the intended buffer when handling certain	https://www.huawei.com/en/psirt/security-advisories/huawei-sa-20200715-03-smartphone-en	H-HUA-P30_-190820/1378

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			operations of certificate, the attacker should trick the user into installing a malicious application, successful exploit may cause code execution. **CVE ID : CVE-2020-9257**		
p30					
Information Exposure	27-Jul-20	4.3	HUAWEI P30 smart phones with versions earlier than 10.1.0.160(C00E160R2P11) have an information exposure vulnerability. The system does not properly authenticate the application that access a specified interface. Attackers can trick users into installing malicious software to exploit this vulnerability and obtain some information about the device. Successful exploit may cause information disclosure. **CVE ID : CVE-2020-9077**	N/A	H-HUA-P30-190820/1379
Improper Input Validation	31-Jul-20	3.3	HUAWEI P30 smartphones with versions earlier than 10.1.0.160(C00E160R2P11) have a denial of service vulnerability. A module does not deal with mal-crafted messages and it leads to memory leak. Attackers can exploit this vulnerability to make the device denial of service.Affected product versions include: HUAWEI	N/A	H-HUA-P30-190820/1380

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			P30 versions Versions earlier than 10.1.0.160(C00E160R2P11). **CVE ID : CVE-2020-9249**		
honor_10					
Improper Input Validation	17-Jul-20	4.3	Huawei Honor 10 smartphones with versions earlier than 10.0.0.178(C00E178R1P4) have a denial of service vulnerability. Certain service in the system does not sufficiently validate certain parameter which is received, the attacker should trick the user into installing a malicious application, successful exploit could cause a denial of service condition. **CVE ID : CVE-2020-9255**	https://www.huawei.com/en/psirt/security-advisories/huawei-sa-20200715-06-smartphone-en	H-HUA-HONO-190820/1381
mate_20_x					
Improper Limitation of a Pathname to a Restricted Directory ('Path Traversal')	17-Jul-20	2.1	HUAWEI Mate 20 versions earlier than 10.1.0.160(C00E160R3P8), HUAWEI Mate 20 X versions earlier than 10.1.0.135(C00E135R2P8), HUAWEI Mate 20 RS versions earlier than 10.1.0.160(C786E160R3P8), and Honor Magic2 smartphones versions earlier than 10.1.0.160(C00E160R2P11) have a path traversal vulnerability. The system does not sufficiently	https://www.huawei.com/en/psirt/security-advisories/huawei-sa-20200715-07-smartphone-en	H-HUA-MATE-190820/1382

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			validate certain pathname from certain process, successful exploit could allow the attacker write files to a crafted path. **CVE ID : CVE-2020-9252**		
mate_20					
Improper Authenticati on	27-Jul-20	2.1	HUAWEI Mate 20 smartphones with versions earlier than 10.1.0.160(C00E160R2P1 1) have an improper authorization vulnerability. The software does not properly restrict certain operation in certain scenario, the attacker should do certain configuration before the user turns on student mode function. Successful exploit could allow the attacker to bypass the limit of student mode function. Affected product versions include: HUAWEI Mate 20 versions Versions earlier than 10.1.0.160(C00E160R3P8) . **CVE ID : CVE-2020-9251**	N/A	H-HUA-MATE-190820/1383
Improper Limitation of a Pathname to a Restricted Directory ('Path Traversal')	17-Jul-20	2.1	HUAWEI Mate 20 versions earlier than 10.1.0.160(C00E160R3P8) , HUAWEI Mate 20 X versions earlier than 10.1.0.135(C00E135R2P8) , HUAWEI Mate 20 RS versions earlier than 10.1.0.160(C786E160R3P	https://ww w.huawei.co m/en/psirt/ security-advisories/h uawei-sa-20200715-07-smartphone-	H-HUA-MATE-190820/1384

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			8), and Honor Magic2 smartphones versions earlier than 10.1.0.160(C00E160R2P11) have a path traversal vulnerability. The system does not sufficiently validate certain pathname from certain process, successful exploit could allow the attacker write files to a crafted path. **CVE ID : CVE-2020-9252**	en	
ngfw_module					
Out-of-bounds Write	18-Jul-20	3.3	There is an out-of-bounds write vulnerability in some products. An unauthenticated attacker crafts malformed packets with specific parameter and sends the packets to the affected products. Due to insufficient validation of packets, which may be exploited to cause the process reboot. Affected product versions include: IPS Module versions V500R005C00, V500R005C10; NGFW Module versions V500R005C00, V500R005C10; Secospace USG6300 versions V500R001C30, V500R001C60, V500R005C00, V500R005C10; Secospace USG6500 versions V500R001C30,	https://www.huawei.com/en/psirt/security-advisories/huawei-sa-20200715-01-outofboundswrite-en	H-HUA-NGFW-190820/1385

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			V500R001C60, V500R005C00, V500R005C10; Secospace USG6600 versions V500R001C30, V500R001C60, V500R005C00, V500R005C10; USG9500 versions V500R001C30, V500R001C60, V500R005C00, V500R005C10 **CVE ID : CVE-2020-9101**		
mate_20_rs					
Improper Limitation of a Pathname to a Restricted Directory ('Path Traversal')	17-Jul-20	2.1	HUAWEI Mate 20 versions earlier than 10.1.0.160(C00E160R3P8), HUAWEI Mate 20 X versions earlier than 10.1.0.135(C00E135R2P8), HUAWEI Mate 20 RS versions earlier than 10.1.0.160(C786E160R3P8), and Honor Magic2 smartphones versions earlier than 10.1.0.160(C00E160R2P11) have a path traversal vulnerability. The system does not sufficiently validate certain pathname from certain process, successful exploit could allow the attacker write files to a crafted path. **CVE ID : CVE-2020-9252**	https://www.huawei.com/en/psirt/security-advisories/huawei-sa-20200715-07-smartphone-en	H-HUA-MATE-190820/1386
usg9500					
Out-of-bounds	18-Jul-20	3.3	There is an out-of-bounds write vulnerability in some	https://www.huawei.co	H-HUA-USG9-190820/1387

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Write			products. An unauthenticated attacker crafts malformed packets with specific parameter and sends the packets to the affected products. Due to insufficient validation of packets, which may be exploited to cause the process reboot. Affected product versions include: IPS Module versions V500R005C00, V500R005C10; NGFW Module versions V500R005C00, V500R005C10; Secospace USG6300 versions V500R001C30, V500R001C60, V500R005C00, V500R005C10; Secospace USG6500 versions V500R001C30, V500R001C60, V500R005C00, V500R005C10; Secospace USG6600 versions V500R001C30, V500R001C60, V500R005C00, V500R005C10; USG9500 versions V500R001C30, V500R001C60, V500R005C00, V500R005C10 **CVE ID : CVE-2020-9101**	m/en/psirt/security-advisories/huawei-sa-20200715-01-outofbounds write-en	
Juniper					
mx2020					
Improper	17-Jul-20	5	When a device running	https://kb.ju	H-JUN-MX20-

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Input Validation			Juniper Networks Junos OS with MPC7, MPC8, or MPC9 line cards installed and the system is configured for inline IP reassembly, used by L2TP, MAP-E, GRE, and IPIP, the packet forwarding engine (PFE) will become disabled upon receipt of small fragments requiring reassembly, generating the following error messages: [LOG: Err] MQSS(2): WO: Packet Error - Error Packets 1, Connection 29 [LOG: Err] eachip_hmcif_rx_intr_handler(7259): EA[2:0]: HMCIF Rx: Injected checksum error detected on WO response - Chunk Address 0x0 [LOG: Err] MQSS(2): DRD: RORD1: CMD reorder ID error - Command 11, Reorder ID 1960, QID 0 [LOG: Err] MQSS(2): DRD: UNROLL0: HMC chunk address error in stage 5 - Chunk Address: 0xc38fb1 [LOG: Notice] Error: /fpc/0/pfe/0/cm/0/MQSS(2)/2/MQSS_CMERROR_DRD_RORD_ENG_INT_REG_CMD_FSM_STATE_ERR (0x2203cc), scope: pfe, category: functional, severity: major, module: MQSS(2), type: DRD_RORD_ENG_INT: CMD FSM State Error	niper.net/JSA11036	190820/1388

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			[LOG: Notice] Performing action cmalarm for error /fpc/0/pfe/0/cm/0/MQSS(2)/2/MQSS_CMERROR_DRD_RORD_ENG_INT_REG_CMD_FSM_STATE_ERR (0x2203cc) in module: MQSS(2) with scope: pfe category: functional level: major [LOG: Notice] Performing action get-state for error /fpc/0/pfe/0/cm/0/MQSS(2)/2/MQSS_CMERROR_DRD_RORD_ENG_INT_REG_CMD_FSM_STATE_ERR (0x2203cc) in module: MQSS(2) with scope: pfe category: functional level: major [LOG: Notice] Performing action disable-pfe for error /fpc/0/pfe/0/cm/0/MQSS(2)/2/MQSS_CMERROR_DRD_RORD_ENG_INT_REG_CMD_FSM_STATE_ERR (0x2203cc) in module: MQSS(2) with scope: pfe category: functional level: major By continuously sending fragmented packets that cannot be reassembled, an attacker can repeatedly disable the PFE causing a sustained Denial of Service (DoS). This issue affects Juniper Networks Junos OS: 17.2 versions prior to 17.2R3-S4 on MX Series; 17.3 versions prior to 17.3R3-		

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			S8 on MX Series; 17.4 versions prior to 17.4R2-S9, 17.4R3-S1 on MX Series; 18.1 versions prior to 18.1R3-S10 on MX Series; 18.2 versions prior to 18.2R2-S6, 18.2R3-S3 on MX Series; 18.2X75 versions prior to 18.2X75-D34, 18.2X75-D41, 18.2X75-D53, 18.2X75-D65, 18.2X75-D430 on MX Series; 18.3 versions prior to 18.3R1-S7, 18.3R2-S4, 18.3R3-S2 on MX Series; 18.4 versions prior to 18.4R1-S6, 18.4R2-S4, 18.4R3 on MX Series; 19.1 versions prior to 19.1R1-S4, 19.1R2-S1, 19.1R3 on MX Series; 19.2 versions prior to 19.2R1-S3, 19.2R2 on MX Series; 19.3 versions prior to 19.3R2-S2, 19.3R3 on MX Series. This issue is specific to inline IP reassembly, introduced in Junos OS 17.2. Versions of Junos OS prior to 17.2 are unaffected by this vulnerability. **CVE ID : CVE-2020-1649**		
Uncontrolled Resource Consumption	17-Jul-20	5	On Juniper Networks Junos MX Series with service card configured, receipt of a stream of specific packets may crash the MS-PIC component on MS-MIC or MS-MPC. By continuously sending	https://kb.juniper.net/JSA11037	H-JUN-MX20-190820/1389

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			these specific packets, an attacker can repeatedly bring down MS-PIC on MS-MIC/MS-MPC causing a prolonged Denial of Service. This issue affects MX Series devices using MS-PIC, MS-MIC or MS-MPC service cards with any service configured. This issue affects Juniper Networks Junos OS on MX Series: 17.2R2-S7; 17.3R3-S4, 17.3R3-S5; 17.4R2-S4 and the subsequent SRs (17.4R2-S5, 17.4R2-S6, etc.); 17.4R3; 18.1R3-S3, 18.1R3-S4, 18.1R3-S5, 18.1R3-S6, 18.1R3-S7, 18.1R3-S8; 18.2R3, 18.2R3-S1, 18.2R3-S2; 18.3R2 and the SRs based on 18.3R2; 18.4R2 and the SRs based on 18.4R2; 19.1R1 and the SRs based on 19.1R1; 19.2R1 and the SRs based on 19.2R1; 19.3R1 and the SRs based on 19.3R1. **CVE ID : CVE-2020-1650**		
Missing Release of Resource after Effective Lifetime	17-Jul-20	3.3	On Juniper Networks MX series, receipt of a stream of specific Layer 2 frames may cause a memory leak resulting in the packet forwarding engine (PFE) on the line card to crash and restart, causing traffic interruption. By continuously sending this stream of specific layer 2	https://kb.juniper.net/JSA11038	H-JUN-MX20-190820/1390

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			frame, an attacker connected to the same broadcast domain can repeatedly crash the PFE, causing a prolonged Denial of Service (DoS). This issue affects Juniper Networks Junos OS on MX Series: 17.2 versions prior to 17.2R3-S4; 17.2X75 versions prior to 17.2X75-D105.19; 17.3 versions prior to 17.3R3-S7; 17.4 versions prior to 17.4R1-S3, 17.4R2; 18.1 versions prior to 18.1R2. This issue does not affect Juniper Networks Junos OS releases prior to 17.2R1. **CVE ID : CVE-2020-1651**		
Uncontrolled Resource Consumption	17-Jul-20	5	When a device running Juniper Networks Junos OS with MPC7, MPC8, or MPC9 line cards installed and the system is configured for inline IP reassembly, used by L2TP, MAP-E, GRE, and IPIP, the packet forwarding engine (PFE) will become disabled upon receipt of large packets requiring fragmentation, generating the following error messages: [LOG: Err] MQSS(0): WO: Packet Error - Error Packets 1, Connection 29 [LOG: Err] eachip_hmcif_rx_intr_handler(7259): EA[0:0]: HMCIF Rx: Injected checksum	https://kb.juniper.net/JSA11041	H-JUN-MX20-190820/1391

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			error detected on WO response - Chunk Address 0x0 [LOG: Err] MQSS(0): DRD: RORD1: CMD reorder ID error - Command 11, Reorder ID 1838, QID 0 [LOG: Err] MQSS(0): DRD: UNROLL0: HMC chunk length error in stage 5 - Chunk Address: 0x4321f3 [LOG: Err] MQSS(0): DRD: UNROLL0: HMC chunk address error in stage 5 - Chunk Address: 0x0 [LOG: Notice] Error: /fpc/8/pfe/0/cm/0/MQSS(0)/0/MQSS_CMERROR_DRD_RORD_ENG_INT_REG_CMD_FSM_STATE_ERR (0x2203cc), scope: pfe, category: functional, severity: major, module: MQSS(0), type: DRD_RORD_ENG_INT: CMD FSM State Error [LOG: Notice] Performing action cmalarm for error /fpc/8/pfe/0/cm/0/MQSS(0)/0/MQSS_CMERROR_DRD_RORD_ENG_INT_REG_CMD_FSM_STATE_ERR (0x2203cc) in module: MQSS(0) with scope: pfe category: functional level: major [LOG: Notice] Performing action get-state for error /fpc/8/pfe/0/cm/0/MQSS(0)/0/MQSS_CMERROR_DRD_RORD_ENG_INT_REG_CMD_FSM_STATE_ERR		

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			(0x2203cc) in module: MQSS(0) with scope: pfe category: functional level: major [LOG: Notice] Performing action disable-pfe for error /fpc/8/pfe/0/cm/0/MQSS(0)/0/MQSS_CMERROR_DRD_RORD_ENG_INT_REG_CMD_FSM_STATE_ERR (0x2203cc) in module: MQSS(0) with scope: pfe category: functional level: major By continuously sending fragmented packets that cannot be reassembled, an attacker can repeatedly disable the PFE causing a sustained Denial of Service (DoS). This issue affects Juniper Networks Junos OS: 17.2 versions prior to 17.2R3-S4 on MX Series; 17.3 versions prior to 17.3R3-S8 on MX Series; 17.4 versions prior to 17.4R2-S10, 17.4R3-S2 on MX Series; 18.1 versions prior to 18.1R3-S10 on MX Series; 18.2 versions prior to 18.2R3-S3 on MX Series; 18.2X75 versions prior to 18.2X75-D41, 18.2X75-D430, 18.2X75-D65 on MX Series; 18.3 versions prior to 18.3R1-S7, 18.3R2-S4, 18.3R3-S1 on MX Series; 18.4 versions prior to 18.4R1-S7, 18.4R2-S4, 18.4R3 on MX Series; 19.1		

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			versions prior to 19.1R1-S5, 19.1R2-S1, 19.1R3 on MX Series; 19.2 versions prior to 19.2R1-S4, 19.2R2 on MX Series; 19.3 versions prior to 19.3R2-S2, 19.3R3 on MX Series. This issue is specific to inline IP reassembly, introduced in Junos OS 17.2. Versions of Junos OS prior to 17.2 are unaffected by this vulnerability. **CVE ID : CVE-2020-1655**		
mx204					
Improper Input Validation	17-Jul-20	5	When a device running Juniper Networks Junos OS with MPC7, MPC8, or MPC9 line cards installed and the system is configured for inline IP reassembly, used by L2TP, MAP-E, GRE, and IPIP, the packet forwarding engine (PFE) will become disabled upon receipt of small fragments requiring reassembly, generating the following error messages: [LOG: Err] MQSS(2): WO: Packet Error - Error Packets 1, Connection 29 [LOG: Err] eachip_hmcif_rx_intr_handler(7259): EA[2:0]: HMCIF Rx: Injected checksum error detected on WO response - Chunk Address 0x0 [LOG: Err] MQSS(2):	https://kb.juniper.net/JSA11036	H-JUN-MX20-190820/1392

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			DRD: RORD1: CMD reorder ID error - Command 11, Reorder ID 1960, QID 0 [LOG: Err] MQSS(2): DRD: UNROLL0: HMC chunk address error in stage 5 - Chunk Address: 0xc38fb1 [LOG: Notice] Error: /fpc/0/pfe/0/cm/0/MQSS(2)/2/MQSS_CMERROR_DRD_RORD_ENG_INT_REG_CMD_FSM_STATE_ERR (0x2203cc), scope: pfe, category: functional, severity: major, module: MQSS(2), type: DRD_RORD_ENG_INT: CMD FSM State Error [LOG: Notice] Performing action cmalarm for error /fpc/0/pfe/0/cm/0/MQSS(2)/2/MQSS_CMERROR_DRD_RORD_ENG_INT_REG_CMD_FSM_STATE_ERR (0x2203cc) in module: MQSS(2) with scope: pfe category: functional level: major [LOG: Notice] Performing action get-state for error /fpc/0/pfe/0/cm/0/MQSS(2)/2/MQSS_CMERROR_DRD_RORD_ENG_INT_REG_CMD_FSM_STATE_ERR (0x2203cc) in module: MQSS(2) with scope: pfe category: functional level: major [LOG: Notice] Performing action disable-pfe for error /fpc/0/pfe/0/cm/0/MQSS		

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			(2)/2/MQSS_CMERROR_DRD_RORD_ENG_INT_REG_CMD_FSM_STATE_ERR (0x2203cc) in module: MQSS(2) with scope: pfe category: functional level: major By continuously sending fragmented packets that cannot be reassembled, an attacker can repeatedly disable the PFE causing a sustained Denial of Service (DoS). This issue affects Juniper Networks Junos OS: 17.2 versions prior to 17.2R3-S4 on MX Series; 17.3 versions prior to 17.3R3-S8 on MX Series; 17.4 versions prior to 17.4R2-S9, 17.4R3-S1 on MX Series; 18.1 versions prior to 18.1R3-S10 on MX Series; 18.2 versions prior to 18.2R2-S6, 18.2R3-S3 on MX Series; 18.2X75 versions prior to 18.2X75-D34, 18.2X75-D41, 18.2X75-D53, 18.2X75-D65, 18.2X75-D430 on MX Series; 18.3 versions prior to 18.3R1-S7, 18.3R2-S4, 18.3R3-S2 on MX Series; 18.4 versions prior to 18.4R1-S6, 18.4R2-S4, 18.4R3 on MX Series; 19.1 versions prior to 19.1R1-S4, 19.1R2-S1, 19.1R3 on MX Series; 19.2 versions prior to 19.2R1-S3, 19.2R2 on MX Series; 19.3		

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			versions prior to 19.3R2-S2, 19.3R3 on MX Series. This issue is specific to inline IP reassembly, introduced in Junos OS 17.2. Versions of Junos OS prior to 17.2 are unaffected by this vulnerability. **CVE ID : CVE-2020-1649**		
Uncontrolled Resource Consumption	17-Jul-20	5	On Juniper Networks Junos MX Series with service card configured, receipt of a stream of specific packets may crash the MS-PIC component on MS-MIC or MS-MPC. By continuously sending these specific packets, an attacker can repeatedly bring down MS-PIC on MS-MIC/MS-MPC causing a prolonged Denial of Service. This issue affects MX Series devices using MS-PIC, MS-MIC or MS-MPC service cards with any service configured. This issue affects Juniper Networks Junos OS on MX Series: 17.2R2-S7; 17.3R3-S4, 17.3R3-S5; 17.4R2-S4 and the subsequent SRs (17.4R2-S5, 17.4R2-S6, etc.); 17.4R3; 18.1R3-S3, 18.1R3-S4, 18.1R3-S5, 18.1R3-S6, 18.1R3-S7, 18.1R3-S8; 18.2R3, 18.2R3-S1, 18.2R3-S2; 18.3R2 and the SRs based on 18.3R2; 18.4R2 and the	https://kb.juniper.net/JSA11037	H-JUN-MX20-190820/1393

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			SRs based on 18.4R2; 19.1R1 and the SRs based on 19.1R1; 19.2R1 and the SRs based on 19.2R1; 19.3R1 and the SRs based on 19.3R1. **CVE ID : CVE-2020-1650**		
Missing Release of Resource after Effective Lifetime	17-Jul-20	3.3	On Juniper Networks MX series, receipt of a stream of specific Layer 2 frames may cause a memory leak resulting in the packet forwarding engine (PFE) on the line card to crash and restart, causing traffic interruption. By continuously sending this stream of specific layer 2 frame, an attacker connected to the same broadcast domain can repeatedly crash the PFE, causing a prolonged Denial of Service (DoS). This issue affects Juniper Networks Junos OS on MX Series: 17.2 versions prior to 17.2R3-S4; 17.2X75 versions prior to 17.2X75-D105.19; 17.3 versions prior to 17.3R3-S7; 17.4 versions prior to 17.4R1-S3, 17.4R2; 18.1 versions prior to 18.1R2. This issue does not affect Juniper Networks Junos OS releases prior to 17.2R1. **CVE ID : CVE-2020-1651**	https://kb.juniper.net/JSA11038	H-JUN-MX20-190820/1394
Uncontrolled Resource	17-Jul-20	5	When a device running Juniper Networks Junos OS	https://kb.juniper.net/JS	H-JUN-MX20-190820/1395

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Consumption			with MPC7, MPC8, or MPC9 line cards installed and the system is configured for inline IP reassembly, used by L2TP, MAP-E, GRE, and IPIP, the packet forwarding engine (PFE) will become disabled upon receipt of large packets requiring fragmentation, generating the following error messages: [LOG: Err] MQSS(0): WO: Packet Error - Error Packets 1, Connection 29 [LOG: Err] eachip_hmcif_rx_intr_handler(7259): EA[0:0]: HMCIF Rx: Injected checksum error detected on WO response - Chunk Address 0x0 [LOG: Err] MQSS(0): DRD: RORD1: CMD reorder ID error - Command 11, Reorder ID 1838, QID 0 [LOG: Err] MQSS(0): DRD: UNROLL0: HMC chunk length error in stage 5 - Chunk Address: 0x4321f3 [LOG: Err] MQSS(0): DRD: UNROLL0: HMC chunk address error in stage 5 - Chunk Address: 0x0 [LOG: Notice] Error: /fpc/8/pfe/0/cm/0/MQSS(0)/0/MQSS_CMERROR_DRD_RORD_ENG_INT_REG_CMD_FSM_STATE_ERR (0x2203cc), scope: pfe, category: functional, severity: major, module:	A11041	

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			MQSS(0), type: DRD_RORD_ENG_INT: CMD FSM State Error [LOG: Notice] Performing action cmalarm for error /fpc/8/pfe/0/cm/0/MQSS(0)/0/MQSS_CMERROR_DRD_RORD_ENG_INT_REG_CMD_FSM_STATE_ERR (0x2203cc) in module: MQSS(0) with scope: pfe category: functional level: major [LOG: Notice] Performing action get-state for error /fpc/8/pfe/0/cm/0/MQSS(0)/0/MQSS_CMERROR_DRD_RORD_ENG_INT_REG_CMD_FSM_STATE_ERR (0x2203cc) in module: MQSS(0) with scope: pfe category: functional level: major [LOG: Notice] Performing action disable-pfe for error /fpc/8/pfe/0/cm/0/MQSS(0)/0/MQSS_CMERROR_DRD_RORD_ENG_INT_REG_CMD_FSM_STATE_ERR (0x2203cc) in module: MQSS(0) with scope: pfe category: functional level: major By continuously sending fragmented packets that cannot be reassembled, an attacker can repeatedly disable the PFE causing a sustained Denial of Service (DoS). This issue affects Juniper Networks Junos OS: 17.2		

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			versions prior to 17.2R3-S4 on MX Series; 17.3 versions prior to 17.3R3-S8 on MX Series; 17.4 versions prior to 17.4R2-S10, 17.4R3-S2 on MX Series; 18.1 versions prior to 18.1R3-S10 on MX Series; 18.2 versions prior to 18.2R3-S3 on MX Series; 18.2X75 versions prior to 18.2X75-D41, 18.2X75-D430, 18.2X75-D65 on MX Series; 18.3 versions prior to 18.3R1-S7, 18.3R2-S4, 18.3R3-S1 on MX Series; 18.4 versions prior to 18.4R1-S7, 18.4R2-S4, 18.4R3 on MX Series; 19.1 versions prior to 19.1R1-S5, 19.1R2-S1, 19.1R3 on MX Series; 19.2 versions prior to 19.2R1-S4, 19.2R2 on MX Series; 19.3 versions prior to 19.3R2-S2, 19.3R3 on MX Series. This issue is specific to inline IP reassembly, introduced in Junos OS 17.2. Versions of Junos OS prior to 17.2 are unaffected by this vulnerability. **CVE ID : CVE-2020-1655**		
mx240					
Improper Input Validation	17-Jul-20	5	When a device running Juniper Networks Junos OS with MPC7, MPC8, or MPC9 line cards installed and the system is	https://kb.juniper.net/JSA11036	H-JUN-MX24-190820/1396

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			configured for inline IP reassembly, used by L2TP, MAP-E, GRE, and IPIP, the packet forwarding engine (PFE) will become disabled upon receipt of small fragments requiring reassembly, generating the following error messages: [LOG: Err] MQSS(2): WO: Packet Error - Error Packets 1, Connection 29 [LOG: Err] eachip_hmcif_rx_intr_handler(7259): EA[2:0]: HMCIF Rx: Injected checksum error detected on WO response - Chunk Address 0x0 [LOG: Err] MQSS(2): DRD: RORD1: CMD reorder ID error - Command 11, Reorder ID 1960, QID 0 [LOG: Err] MQSS(2): DRD: UNROLL0: HMC chunk address error in stage 5 - Chunk Address: 0xc38fb1 [LOG: Notice] Error: /fpc/0/pfe/0/cm/0/MQSS(2)/2/MQSS_CMERROR_DRD_RORD_ENG_INT_REG_CMD_FSM_STATE_ERR (0x2203cc), scope: pfe, category: functional, severity: major, module: MQSS(2), type: DRD_RORD_ENG_INT: CMD FSM State Error [LOG: Notice] Performing action cmalarm for error /fpc/0/pfe/0/cm/0/MQSS(2)/2/MQSS_CMERROR_D		

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			RD_RORD_ENG_INT_REG_CMD_FSM_STATE_ERR (0x2203cc) in module: MQSS(2) with scope: pfe category: functional level: major [LOG: Notice] Performing action get-state for error /fpc/0/pfe/0/cm/0/MQSS(2)/2/MQSS_CMERROR_DRD_RORD_ENG_INT_REG_CMD_FSM_STATE_ERR (0x2203cc) in module: MQSS(2) with scope: pfe category: functional level: major [LOG: Notice] Performing action disable-pfe for error /fpc/0/pfe/0/cm/0/MQSS(2)/2/MQSS_CMERROR_DRD_RORD_ENG_INT_REG_CMD_FSM_STATE_ERR (0x2203cc) in module: MQSS(2) with scope: pfe category: functional level: major By continuously sending fragmented packets that cannot be reassembled, an attacker can repeatedly disable the PFE causing a sustained Denial of Service (DoS). This issue affects Juniper Networks Junos OS: 17.2 versions prior to 17.2R3-S4 on MX Series; 17.3 versions prior to 17.3R3-S8 on MX Series; 17.4 versions prior to 17.4R2-S9, 17.4R3-S1 on MX Series; 18.1 versions prior		

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			to 18.1R3-S10 on MX Series; 18.2 versions prior to 18.2R2-S6, 18.2R3-S3 on MX Series; 18.2X75 versions prior to 18.2X75-D34, 18.2X75-D41, 18.2X75-D53, 18.2X75-D65, 18.2X75-D430 on MX Series; 18.3 versions prior to 18.3R1-S7, 18.3R2-S4, 18.3R3-S2 on MX Series; 18.4 versions prior to 18.4R1-S6, 18.4R2-S4, 18.4R3 on MX Series; 19.1 versions prior to 19.1R1-S4, 19.1R2-S1, 19.1R3 on MX Series; 19.2 versions prior to 19.2R1-S3, 19.2R2 on MX Series; 19.3 versions prior to 19.3R2-S2, 19.3R3 on MX Series. This issue is specific to inline IP reassembly, introduced in Junos OS 17.2. Versions of Junos OS prior to 17.2 are unaffected by this vulnerability. **CVE ID : CVE-2020-1649**		
Uncontrolled Resource Consumption	17-Jul-20	5	On Juniper Networks Junos MX Series with service card configured, receipt of a stream of specific packets may crash the MS-PIC component on MS-MIC or MS-MPC. By continuously sending these specific packets, an attacker can repeatedly bring down MS-PIC on MS-MIC/MS-MPC causing a	https://kb.juniper.net/JSA11037	H-JUN-MX24-190820/1397

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			prolonged Denial of Service. This issue affects MX Series devices using MS-PIC, MS-MIC or MS-MPC service cards with any service configured. This issue affects Juniper Networks Junos OS on MX Series: 17.2R2-S7; 17.3R3-S4, 17.3R3-S5; 17.4R2-S4 and the subsequent SRs (17.4R2-S5, 17.4R2-S6, etc.); 17.4R3; 18.1R3-S3, 18.1R3-S4, 18.1R3-S5, 18.1R3-S6, 18.1R3-S7, 18.1R3-S8; 18.2R3, 18.2R3-S1, 18.2R3-S2; 18.3R2 and the SRs based on 18.3R2; 18.4R2 and the SRs based on 18.4R2; 19.1R1 and the SRs based on 19.1R1; 19.2R1 and the SRs based on 19.2R1; 19.3R1 and the SRs based on 19.3R1. **CVE ID : CVE-2020-1650**		
Missing Release of Resource after Effective Lifetime	17-Jul-20	3.3	On Juniper Networks MX series, receipt of a stream of specific Layer 2 frames may cause a memory leak resulting in the packet forwarding engine (PFE) on the line card to crash and restart, causing traffic interruption. By continuously sending this stream of specific layer 2 frame, an attacker connected to the same broadcast domain can repeatedly crash the PFE,	https://kb.juniper.net/JSA11038	H-JUN-MX24-190820/1398

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			causing a prolonged Denial of Service (DoS). This issue affects Juniper Networks Junos OS on MX Series: 17.2 versions prior to 17.2R3-S4; 17.2X75 versions prior to 17.2X75-D105.19; 17.3 versions prior to 17.3R3-S7; 17.4 versions prior to 17.4R1-S3, 17.4R2; 18.1 versions prior to 18.1R2. This issue does not affect Juniper Networks Junos OS releases prior to 17.2R1. **CVE ID : CVE-2020-1651**		
Uncontrolled Resource Consumption	17-Jul-20	5	When a device running Juniper Networks Junos OS with MPC7, MPC8, or MPC9 line cards installed and the system is configured for inline IP reassembly, used by L2TP, MAP-E, GRE, and IPIP, the packet forwarding engine (PFE) will become disabled upon receipt of large packets requiring fragmentation, generating the following error messages: [LOG: Err] MQSS(0): WO: Packet Error - Error Packets 1, Connection 29 [LOG: Err] eachip_hmcif_rx_intr_handler(7259): EA[0:0]: HMCIF Rx: Injected checksum error detected on WO response - Chunk Address 0x0 [LOG: Err] MQSS(0): DRD: RORD1: CMD reorder	https://kb.juniper.net/JSA11041	H-JUN-MX24-190820/1399

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			ID error - Command 11, Reorder ID 1838, QID 0 [LOG: Err] MQSS(0): DRD: UNROLL0: HMC chunk length error in stage 5 - Chunk Address: 0x4321f3 [LOG: Err] MQSS(0): DRD: UNROLL0: HMC chunk address error in stage 5 - Chunk Address: 0x0 [LOG: Notice] Error: /fpc/8/pfe/0/cm/0/MQSS(0)/0/MQSS_CMERROR_DRD_RORD_ENG_INT_REG_CMD_FSM_STATE_ERR (0x2203cc), scope: pfe, category: functional, severity: major, module: MQSS(0), type: DRD_RORD_ENG_INT: CMD FSM State Error [LOG: Notice] Performing action cmalarm for error /fpc/8/pfe/0/cm/0/MQSS(0)/0/MQSS_CMERROR_DRD_RORD_ENG_INT_REG_CMD_FSM_STATE_ERR (0x2203cc) in module: MQSS(0) with scope: pfe category: functional level: major [LOG: Notice] Performing action get-state for error /fpc/8/pfe/0/cm/0/MQSS(0)/0/MQSS_CMERROR_DRD_RORD_ENG_INT_REG_CMD_FSM_STATE_ERR (0x2203cc) in module: MQSS(0) with scope: pfe category: functional level: major [LOG: Notice]		

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Performing action disable-pfe for error /fpc/8/pfe/0/cm/0/MQSS(0)/0/MQSS_CMERROR_DRD_RORD_ENG_INT_REG_CMD_FSM_STATE_ERR (0x2203cc) in module: MQSS(0) with scope: pfe category: functional level: major By continuously sending fragmented packets that cannot be reassembled, an attacker can repeatedly disable the PFE causing a sustained Denial of Service (DoS). This issue affects Juniper Networks Junos OS: 17.2 versions prior to 17.2R3-S4 on MX Series; 17.3 versions prior to 17.3R3-S8 on MX Series; 17.4 versions prior to 17.4R2-S10, 17.4R3-S2 on MX Series; 18.1 versions prior to 18.1R3-S10 on MX Series; 18.2 versions prior to 18.2R3-S3 on MX Series; 18.2X75 versions prior to 18.2X75-D41, 18.2X75-D430, 18.2X75-D65 on MX Series; 18.3 versions prior to 18.3R1-S7, 18.3R2-S4, 18.3R3-S1 on MX Series; 18.4 versions prior to 18.4R1-S7, 18.4R2-S4, 18.4R3 on MX Series; 19.1 versions prior to 19.1R1-S5, 19.1R2-S1, 19.1R3 on MX Series; 19.2 versions prior to 19.2R1-S4, 19.2R2		

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			on MX Series; 19.3 versions prior to 19.3R2-S2, 19.3R3 on MX Series. This issue is specific to inline IP reassembly, introduced in Junos OS 17.2. Versions of Junos OS prior to 17.2 are unaffected by this vulnerability. **CVE ID : CVE-2020-1655**		
mx40					
Improper Input Validation	17-Jul-20	5	When a device running Juniper Networks Junos OS with MPC7, MPC8, or MPC9 line cards installed and the system is configured for inline IP reassembly, used by L2TP, MAP-E, GRE, and IPIP, the packet forwarding engine (PFE) will become disabled upon receipt of small fragments requiring reassembly, generating the following error messages: [LOG: Err] MQSS(2): WO: Packet Error - Error Packets 1, Connection 29 [LOG: Err] eachip_hmcif_rx_intr_handler(7259): EA[2:0]: HMCIF Rx: Injected checksum error detected on WO response - Chunk Address 0x0 [LOG: Err] MQSS(2): DRD: RORD1: CMD reorder ID error - Command 11, Reorder ID 1960, QID 0 [LOG: Err] MQSS(2): DRD:	https://kb.juniper.net/JSA11036	H-JUN-MX40-190820/1400

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			UNROLL0: HMC chunk address error in stage 5 - Chunk Address: 0xc38fb1 [LOG: Notice] Error: /fpc/0/pfe/0/cm/0/MQSS(2)/2/MQSS_CMERROR_DRD_RORD_ENG_INT_REG_CMD_FSM_STATE_ERR (0x2203cc), scope: pfe, category: functional, severity: major, module: MQSS(2), type: DRD_RORD_ENG_INT: CMD FSM State Error [LOG: Notice] Performing action cmalarm for error /fpc/0/pfe/0/cm/0/MQSS(2)/2/MQSS_CMERROR_DRD_RORD_ENG_INT_REG_CMD_FSM_STATE_ERR (0x2203cc) in module: MQSS(2) with scope: pfe category: functional level: major [LOG: Notice] Performing action get-state for error /fpc/0/pfe/0/cm/0/MQSS(2)/2/MQSS_CMERROR_DRD_RORD_ENG_INT_REG_CMD_FSM_STATE_ERR (0x2203cc) in module: MQSS(2) with scope: pfe category: functional level: major [LOG: Notice] Performing action disable-pfe for error /fpc/0/pfe/0/cm/0/MQSS(2)/2/MQSS_CMERROR_DRD_RORD_ENG_INT_REG_CMD_FSM_STATE_ERR (0x2203cc) in module:		

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			MQSS(2) with scope: pfe category: functional level: major By continuously sending fragmented packets that cannot be reassembled, an attacker can repeatedly disable the PFE causing a sustained Denial of Service (DoS). This issue affects Juniper Networks Junos OS: 17.2 versions prior to 17.2R3-S4 on MX Series; 17.3 versions prior to 17.3R3-S8 on MX Series; 17.4 versions prior to 17.4R2-S9, 17.4R3-S1 on MX Series; 18.1 versions prior to 18.1R3-S10 on MX Series; 18.2 versions prior to 18.2R2-S6, 18.2R3-S3 on MX Series; 18.2X75 versions prior to 18.2X75-D34, 18.2X75-D41, 18.2X75-D53, 18.2X75-D65, 18.2X75-D430 on MX Series; 18.3 versions prior to 18.3R1-S7, 18.3R2-S4, 18.3R3-S2 on MX Series; 18.4 versions prior to 18.4R1-S6, 18.4R2-S4, 18.4R3 on MX Series; 19.1 versions prior to 19.1R1-S4, 19.1R2-S1, 19.1R3 on MX Series; 19.2 versions prior to 19.2R1-S3, 19.2R2 on MX Series; 19.3 versions prior to 19.3R2-S2, 19.3R3 on MX Series. This issue is specific to inline IP reassembly,		

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			introduced in Junos OS 17.2. Versions of Junos OS prior to 17.2 are unaffected by this vulnerability. **CVE ID : CVE-2020-1649**		
Uncontrolled Resource Consumption	17-Jul-20	5	On Juniper Networks Junos MX Series with service card configured, receipt of a stream of specific packets may crash the MS-PIC component on MS-MIC or MS-MPC. By continuously sending these specific packets, an attacker can repeatedly bring down MS-PIC on MS-MIC/MS-MPC causing a prolonged Denial of Service. This issue affects MX Series devices using MS-PIC, MS-MIC or MS-MPC service cards with any service configured. This issue affects Juniper Networks Junos OS on MX Series: 17.2R2-S7; 17.3R3-S4, 17.3R3-S5; 17.4R2-S4 and the subsequent SRs (17.4R2-S5, 17.4R2-S6, etc.); 17.4R3; 18.1R3-S3, 18.1R3-S4, 18.1R3-S5, 18.1R3-S6, 18.1R3-S7, 18.1R3-S8; 18.2R3, 18.2R3-S1, 18.2R3-S2; 18.3R2 and the SRs based on 18.3R2; 18.4R2 and the SRs based on 18.4R2; 19.1R1 and the SRs based on 19.1R1; 19.2R1 and the SRs based on 19.2R1;	https://kb.juniper.net/JSA11037	H-JUN-MX40-190820/1401

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			19.3R1 and the SRs based on 19.3R1. **CVE ID : CVE-2020-1650**		
Missing Release of Resource after Effective Lifetime	17-Jul-20	3.3	On Juniper Networks MX series, receipt of a stream of specific Layer 2 frames may cause a memory leak resulting in the packet forwarding engine (PFE) on the line card to crash and restart, causing traffic interruption. By continuously sending this stream of specific layer 2 frame, an attacker connected to the same broadcast domain can repeatedly crash the PFE, causing a prolonged Denial of Service (DoS). This issue affects Juniper Networks Junos OS on MX Series: 17.2 versions prior to 17.2R3-S4; 17.2X75 versions prior to 17.2X75-D105.19; 17.3 versions prior to 17.3R3-S7; 17.4 versions prior to 17.4R1-S3, 17.4R2; 18.1 versions prior to 18.1R2. This issue does not affect Juniper Networks Junos OS releases prior to 17.2R1. **CVE ID : CVE-2020-1651**	https://kb.juniper.net/JSA11038	H-JUN-MX40-190820/1402
Uncontrolled Resource Consumption	17-Jul-20	5	When a device running Juniper Networks Junos OS with MPC7, MPC8, or MPC9 line cards installed and the system is configured for inline IP	https://kb.juniper.net/JSA11041	H-JUN-MX40-190820/1403

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			reassembly, used by L2TP, MAP-E, GRE, and IPIP, the packet forwarding engine (PFE) will become disabled upon receipt of large packets requiring fragmentation, generating the following error messages: [LOG: Err] MQSS(0): WO: Packet Error - Error Packets 1, Connection 29 [LOG: Err] eachip_hmcif_rx_intr_handler(7259): EA[0:0]: HMCIF Rx: Injected checksum error detected on WO response - Chunk Address 0x0 [LOG: Err] MQSS(0): DRD: RORD1: CMD reorder ID error - Command 11, Reorder ID 1838, QID 0 [LOG: Err] MQSS(0): DRD: UNROLL0: HMC chunk length error in stage 5 - Chunk Address: 0x4321f3 [LOG: Err] MQSS(0): DRD: UNROLL0: HMC chunk address error in stage 5 - Chunk Address: 0x0 [LOG: Notice] Error: /fpc/8/pfe/0/cm/0/MQSS(0)/0/MQSS_CMERROR_DRD_RORD_ENG_INT_REG_CMD_FSM_STATE_ERR (0x2203cc), scope: pfe, category: functional, severity: major, module: MQSS(0), type: DRD_RORD_ENG_INT: CMD FSM State Error [LOG: Notice] Performing		

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			action cmalarm for error /fpc/8/pfe/0/cm/0/MQSS(0)/0/MQSS_CMERROR_DRD_RORD_ENG_INT_REG_CMD_FSM_STATE_ERR (0x2203cc) in module: MQSS(0) with scope: pfe category: functional level: major [LOG: Notice] Performing action get-state for error /fpc/8/pfe/0/cm/0/MQSS(0)/0/MQSS_CMERROR_DRD_RORD_ENG_INT_REG_CMD_FSM_STATE_ERR (0x2203cc) in module: MQSS(0) with scope: pfe category: functional level: major [LOG: Notice] Performing action disable-pfe for error /fpc/8/pfe/0/cm/0/MQSS(0)/0/MQSS_CMERROR_DRD_RORD_ENG_INT_REG_CMD_FSM_STATE_ERR (0x2203cc) in module: MQSS(0) with scope: pfe category: functional level: major By continuously sending fragmented packets that cannot be reassembled, an attacker can repeatedly disable the PFE causing a sustained Denial of Service (DoS). This issue affects Juniper Networks Junos OS: 17.2 versions prior to 17.2R3-S4 on MX Series; 17.3 versions prior to 17.3R3-S8 on MX Series; 17.4		

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			versions prior to 17.4R2-S10, 17.4R3-S2 on MX Series; 18.1 versions prior to 18.1R3-S10 on MX Series; 18.2 versions prior to 18.2R3-S3 on MX Series; 18.2X75 versions prior to 18.2X75-D41, 18.2X75-D430, 18.2X75-D65 on MX Series; 18.3 versions prior to 18.3R1-S7, 18.3R2-S4, 18.3R3-S1 on MX Series; 18.4 versions prior to 18.4R1-S7, 18.4R2-S4, 18.4R3 on MX Series; 19.1 versions prior to 19.1R1-S5, 19.1R2-S1, 19.1R3 on MX Series; 19.2 versions prior to 19.2R1-S4, 19.2R2 on MX Series; 19.3 versions prior to 19.3R2-S2, 19.3R3 on MX Series. This issue is specific to inline IP reassembly, introduced in Junos OS 17.2. Versions of Junos OS prior to 17.2 are unaffected by this vulnerability. **CVE ID : CVE-2020-1655**		
mx480					
Improper Input Validation	17-Jul-20	5	When a device running Juniper Networks Junos OS with MPC7, MPC8, or MPC9 line cards installed and the system is configured for inline IP reassembly, used by L2TP, MAP-E, GRE, and IPIP, the packet forwarding engine	https://kb.juniper.net/JSA11036	H-JUN-MX48-190820/1404

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			(PFE) will become disabled upon receipt of small fragments requiring reassembly, generating the following error messages: [LOG: Err] MQSS(2): WO: Packet Error - Error Packets 1, Connection 29 [LOG: Err] eachip_hmcif_rx_intr_handler(7259): EA[2:0]: HMCIF Rx: Injected checksum error detected on WO response - Chunk Address 0x0 [LOG: Err] MQSS(2): DRD: RORD1: CMD reorder ID error - Command 11, Reorder ID 1960, QID 0 [LOG: Err] MQSS(2): DRD: UNROLL0: HMC chunk address error in stage 5 - Chunk Address: 0xc38fb1 [LOG: Notice] Error: /fpc/0/pfe/0/cm/0/MQSS(2)/2/MQSS_CMERROR_DRD_RORD_ENG_INT_REG_CMD_FSM_STATE_ERR (0x2203cc), scope: pfe, category: functional, severity: major, module: MQSS(2), type: DRD_RORD_ENG_INT: CMD FSM State Error [LOG: Notice] Performing action cmalarm for error /fpc/0/pfe/0/cm/0/MQSS(2)/2/MQSS_CMERROR_DRD_RORD_ENG_INT_REG_CMD_FSM_STATE_ERR (0x2203cc) in module: MQSS(2) with scope: pfe		

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			category: functional level: major [LOG: Notice] Performing action get-state for error /fpc/0/pfe/0/cm/0/MQSS(2)/2/MQSS_CMERROR_DRD_RORD_ENG_INT_REG_CMD_FSM_STATE_ERR (0x2203cc) in module: MQSS(2) with scope: pfe category: functional level: major [LOG: Notice] Performing action disable-pfe for error /fpc/0/pfe/0/cm/0/MQSS(2)/2/MQSS_CMERROR_DRD_RORD_ENG_INT_REG_CMD_FSM_STATE_ERR (0x2203cc) in module: MQSS(2) with scope: pfe category: functional level: major By continuously sending fragmented packets that cannot be reassembled, an attacker can repeatedly disable the PFE causing a sustained Denial of Service (DoS). This issue affects Juniper Networks Junos OS: 17.2 versions prior to 17.2R3-S4 on MX Series; 17.3 versions prior to 17.3R3-S8 on MX Series; 17.4 versions prior to 17.4R2-S9, 17.4R3-S1 on MX Series; 18.1 versions prior to 18.1R3-S10 on MX Series; 18.2 versions prior to 18.2R2-S6, 18.2R3-S3 on MX Series; 18.2X75		

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			versions prior to 18.2X75-D34, 18.2X75-D41, 18.2X75-D53, 18.2X75-D65, 18.2X75-D430 on MX Series; 18.3 versions prior to 18.3R1-S7, 18.3R2-S4, 18.3R3-S2 on MX Series; 18.4 versions prior to 18.4R1-S6, 18.4R2-S4, 18.4R3 on MX Series; 19.1 versions prior to 19.1R1-S4, 19.1R2-S1, 19.1R3 on MX Series; 19.2 versions prior to 19.2R1-S3, 19.2R2 on MX Series; 19.3 versions prior to 19.3R2-S2, 19.3R3 on MX Series. This issue is specific to inline IP reassembly, introduced in Junos OS 17.2. Versions of Junos OS prior to 17.2 are unaffected by this vulnerability. **CVE ID : CVE-2020-1649**		
Uncontrolled Resource Consumption	17-Jul-20	5	On Juniper Networks Junos MX Series with service card configured, receipt of a stream of specific packets may crash the MS-PIC component on MS-MIC or MS-MPC. By continuously sending these specific packets, an attacker can repeatedly bring down MS-PIC on MS-MIC/MS-MPC causing a prolonged Denial of Service. This issue affects MX Series devices using MS-PIC, MS-MIC or MS-	https://kb.juniper.net/JSA11037	H-JUN-MX48-190820/1405

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			MPC service cards with any service configured. This issue affects Juniper Networks Junos OS on MX Series: 17.2R2-S7; 17.3R3-S4, 17.3R3-S5; 17.4R2-S4 and the subsequent SRs (17.4R2-S5, 17.4R2-S6, etc.); 17.4R3; 18.1R3-S3, 18.1R3-S4, 18.1R3-S5, 18.1R3-S6, 18.1R3-S7, 18.1R3-S8; 18.2R3, 18.2R3-S1, 18.2R3-S2; 18.3R2 and the SRs based on 18.3R2; 18.4R2 and the SRs based on 18.4R2; 19.1R1 and the SRs based on 19.1R1; 19.2R1 and the SRs based on 19.2R1; 19.3R1 and the SRs based on 19.3R1. **CVE ID : CVE-2020-1650**		
Missing Release of Resource after Effective Lifetime	17-Jul-20	3.3	On Juniper Networks MX series, receipt of a stream of specific Layer 2 frames may cause a memory leak resulting in the packet forwarding engine (PFE) on the line card to crash and restart, causing traffic interruption. By continuously sending this stream of specific layer 2 frame, an attacker connected to the same broadcast domain can repeatedly crash the PFE, causing a prolonged Denial of Service (DoS). This issue affects Juniper Networks Junos OS on MX Series:	https://kb.juniper.net/JSA11038	H-JUN-MX48-190820/1406

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			17.2 versions prior to 17.2R3-S4; 17.2X75 versions prior to 17.2X75-D105.19; 17.3 versions prior to 17.3R3-S7; 17.4 versions prior to 17.4R1-S3, 17.4R2; 18.1 versions prior to 18.1R2. This issue does not affect Juniper Networks Junos OS releases prior to 17.2R1. **CVE ID : CVE-2020-1651**		
Uncontrolled Resource Consumption	17-Jul-20	5	When a device running Juniper Networks Junos OS with MPC7, MPC8, or MPC9 line cards installed and the system is configured for inline IP reassembly, used by L2TP, MAP-E, GRE, and IPIP, the packet forwarding engine (PFE) will become disabled upon receipt of large packets requiring fragmentation, generating the following error messages: [LOG: Err] MQSS(0): WO: Packet Error - Error Packets 1, Connection 29 [LOG: Err] eachip_hmcif_rx_intr_handler(7259): EA[0:0]: HMCIF Rx: Injected checksum error detected on WO response - Chunk Address 0x0 [LOG: Err] MQSS(0): DRD: RORD1: CMD reorder ID error - Command 11, Reorder ID 1838, QID 0 [LOG: Err] MQSS(0): DRD: UNROLL0: HMC chunk	https://kb.juniper.net/JSA11041	H-JUN-MX48-190820/1407

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			length error in stage 5 - Chunk Address: 0x4321f3 [LOG: Err] MQSS(0): DRD: UNROLL0: HMC chunk address error in stage 5 - Chunk Address: 0x0 [LOG: Notice] Error: /fpc/8/pfe/0/cm/0/MQSS(0)/0/MQSS_CMERROR_DRD_RORD_ENG_INT_REG_CMD_FSM_STATE_ERR (0x2203cc), scope: pfe, category: functional, severity: major, module: MQSS(0), type: DRD_RORD_ENG_INT: CMD FSM State Error [LOG: Notice] Performing action cmalarm for error /fpc/8/pfe/0/cm/0/MQSS(0)/0/MQSS_CMERROR_DRD_RORD_ENG_INT_REG_CMD_FSM_STATE_ERR (0x2203cc) in module: MQSS(0) with scope: pfe category: functional level: major [LOG: Notice] Performing action get-state for error /fpc/8/pfe/0/cm/0/MQSS(0)/0/MQSS_CMERROR_DRD_RORD_ENG_INT_REG_CMD_FSM_STATE_ERR (0x2203cc) in module: MQSS(0) with scope: pfe category: functional level: major [LOG: Notice] Performing action disable-pfe for error /fpc/8/pfe/0/cm/0/MQSS(0)/0/MQSS_CMERROR_D		

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			RD_RORD_ENG_INT_REG_CMD_FSM_STATE_ERR (0x2203cc) in module: MQSS(0) with scope: pfe category: functional level: major By continuously sending fragmented packets that cannot be reassembled, an attacker can repeatedly disable the PFE causing a sustained Denial of Service (DoS). This issue affects Juniper Networks Junos OS: 17.2 versions prior to 17.2R3-S4 on MX Series; 17.3 versions prior to 17.3R3-S8 on MX Series; 17.4 versions prior to 17.4R2-S10, 17.4R3-S2 on MX Series; 18.1 versions prior to 18.1R3-S10 on MX Series; 18.2 versions prior to 18.2R3-S3 on MX Series; 18.2X75 versions prior to 18.2X75-D41, 18.2X75-D430, 18.2X75-D65 on MX Series; 18.3 versions prior to 18.3R1-S7, 18.3R2-S4, 18.3R3-S1 on MX Series; 18.4 versions prior to 18.4R1-S7, 18.4R2-S4, 18.4R3 on MX Series; 19.1 versions prior to 19.1R1-S5, 19.1R2-S1, 19.1R3 on MX Series; 19.2 versions prior to 19.2R1-S4, 19.2R2 on MX Series; 19.3 versions prior to 19.3R2-S2, 19.3R3 on MX Series. This issue is specific to		

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			inline IP reassembly, introduced in Junos OS 17.2. Versions of Junos OS prior to 17.2 are unaffected by this vulnerability. **CVE ID : CVE-2020-1655**		
mx5					
Improper Input Validation	17-Jul-20	5	When a device running Juniper Networks Junos OS with MPC7, MPC8, or MPC9 line cards installed and the system is configured for inline IP reassembly, used by L2TP, MAP-E, GRE, and IPIP, the packet forwarding engine (PFE) will become disabled upon receipt of small fragments requiring reassembly, generating the following error messages: [LOG: Err] MQSS(2): WO: Packet Error - Error Packets 1, Connection 29 [LOG: Err] eachip_hmcif_rx_intr_handler(7259): EA[2:0]: HMCIF Rx: Injected checksum error detected on WO response - Chunk Address 0x0 [LOG: Err] MQSS(2): DRD: RORD1: CMD reorder ID error - Command 11, Reorder ID 1960, QID 0 [LOG: Err] MQSS(2): DRD: UNROLL0: HMC chunk address error in stage 5 - Chunk Address: 0xc38fb1 [LOG: Notice] Error:	https://kb.juniper.net/JSA11036	H-JUN-MX5-190820/1408

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			/fpc/0/pfe/0/cm/0/MQSS(2)/2/MQSS_CMERROR_DRD_RORD_ENG_INT_REG_CMD_FSM_STATE_ERR (0x2203cc), scope: pfe, category: functional, severity: major, module: MQSS(2), type: DRD_RORD_ENG_INT: CMD FSM State Error [LOG: Notice] Performing action cmalarm for error /fpc/0/pfe/0/cm/0/MQSS(2)/2/MQSS_CMERROR_DRD_RORD_ENG_INT_REG_CMD_FSM_STATE_ERR (0x2203cc) in module: MQSS(2) with scope: pfe category: functional level: major [LOG: Notice] Performing action get-state for error /fpc/0/pfe/0/cm/0/MQSS(2)/2/MQSS_CMERROR_DRD_RORD_ENG_INT_REG_CMD_FSM_STATE_ERR (0x2203cc) in module: MQSS(2) with scope: pfe category: functional level: major [LOG: Notice] Performing action disable-pfe for error /fpc/0/pfe/0/cm/0/MQSS(2)/2/MQSS_CMERROR_DRD_RORD_ENG_INT_REG_CMD_FSM_STATE_ERR (0x2203cc) in module: MQSS(2) with scope: pfe category: functional level: major By continuously sending fragmented		

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			packets that cannot be reassembled, an attacker can repeatedly disable the PFE causing a sustained Denial of Service (DoS). This issue affects Juniper Networks Junos OS: 17.2 versions prior to 17.2R3-S4 on MX Series; 17.3 versions prior to 17.3R3-S8 on MX Series; 17.4 versions prior to 17.4R2-S9, 17.4R3-S1 on MX Series; 18.1 versions prior to 18.1R3-S10 on MX Series; 18.2 versions prior to 18.2R2-S6, 18.2R3-S3 on MX Series; 18.2X75 versions prior to 18.2X75-D34, 18.2X75-D41, 18.2X75-D53, 18.2X75-D65, 18.2X75-D430 on MX Series; 18.3 versions prior to 18.3R1-S7, 18.3R2-S4, 18.3R3-S2 on MX Series; 18.4 versions prior to 18.4R1-S6, 18.4R2-S4, 18.4R3 on MX Series; 19.1 versions prior to 19.1R1-S4, 19.1R2-S1, 19.1R3 on MX Series; 19.2 versions prior to 19.2R1-S3, 19.2R2 on MX Series; 19.3 versions prior to 19.3R2-S2, 19.3R3 on MX Series. This issue is specific to inline IP reassembly, introduced in Junos OS 17.2. Versions of Junos OS prior to 17.2 are unaffected by this		

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			vulnerability. **CVE ID : CVE-2020-1649**		
Uncontrolled Resource Consumption	17-Jul-20	5	On Juniper Networks Junos MX Series with service card configured, receipt of a stream of specific packets may crash the MS-PIC component on MS-MIC or MS-MPC. By continuously sending these specific packets, an attacker can repeatedly bring down MS-PIC on MS-MIC/MS-MPC causing a prolonged Denial of Service. This issue affects MX Series devices using MS-PIC, MS-MIC or MS-MPC service cards with any service configured. This issue affects Juniper Networks Junos OS on MX Series: 17.2R2-S7; 17.3R3-S4, 17.3R3-S5; 17.4R2-S4 and the subsequent SRs (17.4R2-S5, 17.4R2-S6, etc.); 17.4R3; 18.1R3-S3, 18.1R3-S4, 18.1R3-S5, 18.1R3-S6, 18.1R3-S7, 18.1R3-S8; 18.2R3, 18.2R3-S1, 18.2R3-S2; 18.3R2 and the SRs based on 18.3R2; 18.4R2 and the SRs based on 18.4R2; 19.1R1 and the SRs based on 19.1R1; 19.2R1 and the SRs based on 19.2R1; 19.3R1 and the SRs based on 19.3R1. **CVE ID : CVE-2020-1650**	https://kb.juniper.net/JSA11037	H-JUN-MX5-190820/1409

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Missing Release of Resource after Effective Lifetime	17-Jul-20	3.3	On Juniper Networks MX series, receipt of a stream of specific Layer 2 frames may cause a memory leak resulting in the packet forwarding engine (PFE) on the line card to crash and restart, causing traffic interruption. By continuously sending this stream of specific layer 2 frame, an attacker connected to the same broadcast domain can repeatedly crash the PFE, causing a prolonged Denial of Service (DoS). This issue affects Juniper Networks Junos OS on MX Series: 17.2 versions prior to 17.2R3-S4; 17.2X75 versions prior to 17.2X75-D105.19; 17.3 versions prior to 17.3R3-S7; 17.4 versions prior to 17.4R1-S3, 17.4R2; 18.1 versions prior to 18.1R2. This issue does not affect Juniper Networks Junos OS releases prior to 17.2R1. **CVE ID : CVE-2020-1651**	https://kb.juniper.net/JSA11038	H-JUN-MX5-190820/1410
Uncontrolled Resource Consumption	17-Jul-20	5	When a device running Juniper Networks Junos OS with MPC7, MPC8, or MPC9 line cards installed and the system is configured for inline IP reassembly, used by L2TP, MAP-E, GRE, and IPIP, the packet forwarding engine (PFE) will become	https://kb.juniper.net/JSA11041	H-JUN-MX5-190820/1411

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			disabled upon receipt of large packets requiring fragmentation, generating the following error messages: [LOG: Err] MQSS(0): WO: Packet Error - Error Packets 1, Connection 29 [LOG: Err] eachip_hmcif_rx_intr_handler(7259): EA[0:0]: HMCIF Rx: Injected checksum error detected on WO response - Chunk Address 0x0 [LOG: Err] MQSS(0): DRD: RORD1: CMD reorder ID error - Command 11, Reorder ID 1838, QID 0 [LOG: Err] MQSS(0): DRD: UNROLL0: HMC chunk length error in stage 5 - Chunk Address: 0x4321f3 [LOG: Err] MQSS(0): DRD: UNROLL0: HMC chunk address error in stage 5 - Chunk Address: 0x0 [LOG: Notice] Error: /fpc/8/pfe/0/cm/0/MQSS(0)/0/MQSS_CMERROR_DRD_RORD_ENG_INT_REG_CMD_FSM_STATE_ERR (0x2203cc), scope: pfe, category: functional, severity: major, module: MQSS(0), type: DRD_RORD_ENG_INT: CMD FSM State Error [LOG: Notice] Performing action cmalarm for error /fpc/8/pfe/0/cm/0/MQSS(0)/0/MQSS_CMERROR_DRD_RORD_ENG_INT_REG_C		

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			MD_FSM_STATE_ERR (0x2203cc) in module: MQSS(0) with scope: pfe category: functional level: major [LOG: Notice] Performing action get-state for error /fpc/8/pfe/0/cm/0/MQSS(0)/0/MQSS_CMERROR_DRD_RORD_ENG_INT_REG_CMD_FSM_STATE_ERR (0x2203cc) in module: MQSS(0) with scope: pfe category: functional level: major [LOG: Notice] Performing action disable-pfe for error /fpc/8/pfe/0/cm/0/MQSS(0)/0/MQSS_CMERROR_DRD_RORD_ENG_INT_REG_CMD_FSM_STATE_ERR (0x2203cc) in module: MQSS(0) with scope: pfe category: functional level: major By continuously sending fragmented packets that cannot be reassembled, an attacker can repeatedly disable the PFE causing a sustained Denial of Service (DoS). This issue affects Juniper Networks Junos OS: 17.2 versions prior to 17.2R3-S4 on MX Series; 17.3 versions prior to 17.3R3-S8 on MX Series; 17.4 versions prior to 17.4R2-S10, 17.4R3-S2 on MX Series; 18.1 versions prior to 18.1R3-S10 on MX		

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Series; 18.2 versions prior to 18.2R3-S3 on MX Series; 18.2X75 versions prior to 18.2X75-D41, 18.2X75-D430, 18.2X75-D65 on MX Series; 18.3 versions prior to 18.3R1-S7, 18.3R2-S4, 18.3R3-S1 on MX Series; 18.4 versions prior to 18.4R1-S7, 18.4R2-S4, 18.4R3 on MX Series; 19.1 versions prior to 19.1R1-S5, 19.1R2-S1, 19.1R3 on MX Series; 19.2 versions prior to 19.2R1-S4, 19.2R2 on MX Series; 19.3 versions prior to 19.3R2-S2, 19.3R3 on MX Series. This issue is specific to inline IP reassembly, introduced in Junos OS 17.2. Versions of Junos OS prior to 17.2 are unaffected by this vulnerability. **CVE ID : CVE-2020-1655**		
mx80					
Improper Input Validation	17-Jul-20	5	When a device running Juniper Networks Junos OS with MPC7, MPC8, or MPC9 line cards installed and the system is configured for inline IP reassembly, used by L2TP, MAP-E, GRE, and IPIP, the packet forwarding engine (PFE) will become disabled upon receipt of small fragments requiring reassembly, generating the	https://kb.juniper.net/JSA11036	H-JUN-MX80-190820/1412

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			following error messages: [LOG: Err] MQSS(2): WO: Packet Error - Error Packets 1, Connection 29 [LOG: Err] eachip_hmcif_rx_intr_handler(7259): EA[2:0]: HMCIF Rx: Injected checksum error detected on WO response - Chunk Address 0x0 [LOG: Err] MQSS(2): DRD: RORD1: CMD reorder ID error - Command 11, Reorder ID 1960, QID 0 [LOG: Err] MQSS(2): DRD: UNROLL0: HMC chunk address error in stage 5 - Chunk Address: 0xc38fb1 [LOG: Notice] Error: /fpc/0/pfe/0/cm/0/MQSS(2)/2/MQSS_CMERROR_DRD_RORD_ENG_INT_REG_CMD_FSM_STATE_ERR (0x2203cc), scope: pfe, category: functional, severity: major, module: MQSS(2), type: DRD_RORD_ENG_INT: CMD FSM State Error [LOG: Notice] Performing action cmalarm for error /fpc/0/pfe/0/cm/0/MQSS(2)/2/MQSS_CMERROR_DRD_RORD_ENG_INT_REG_CMD_FSM_STATE_ERR (0x2203cc) in module: MQSS(2) with scope: pfe category: functional level: major [LOG: Notice] Performing action get-state for error		

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			/fpc/0/pfe/0/cm/0/MQSS(2)/2/MQSS_CMERROR_DRD_RORD_ENG_INT_REG_CMD_FSM_STATE_ERR (0x2203cc) in module: MQSS(2) with scope: pfe category: functional level: major [LOG: Notice] Performing action disable-pfe for error /fpc/0/pfe/0/cm/0/MQSS(2)/2/MQSS_CMERROR_DRD_RORD_ENG_INT_REG_CMD_FSM_STATE_ERR (0x2203cc) in module: MQSS(2) with scope: pfe category: functional level: major By continuously sending fragmented packets that cannot be reassembled, an attacker can repeatedly disable the PFE causing a sustained Denial of Service (DoS). This issue affects Juniper Networks Junos OS: 17.2 versions prior to 17.2R3-S4 on MX Series; 17.3 versions prior to 17.3R3-S8 on MX Series; 17.4 versions prior to 17.4R2-S9, 17.4R3-S1 on MX Series; 18.1 versions prior to 18.1R3-S10 on MX Series; 18.2 versions prior to 18.2R2-S6, 18.2R3-S3 on MX Series; 18.2X75 versions prior to 18.2X75-D34, 18.2X75-D41, 18.2X75-D53, 18.2X75-D65, 18.2X75-D430 on MX		

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Series; 18.3 versions prior to 18.3R1-S7, 18.3R2-S4, 18.3R3-S2 on MX Series; 18.4 versions prior to 18.4R1-S6, 18.4R2-S4, 18.4R3 on MX Series; 19.1 versions prior to 19.1R1-S4, 19.1R2-S1, 19.1R3 on MX Series; 19.2 versions prior to 19.2R1-S3, 19.2R2 on MX Series; 19.3 versions prior to 19.3R2-S2, 19.3R3 on MX Series. This issue is specific to inline IP reassembly, introduced in Junos OS 17.2. Versions of Junos OS prior to 17.2 are unaffected by this vulnerability. **CVE ID : CVE-2020-1649**		
Uncontrolled Resource Consumption	17-Jul-20	5	On Juniper Networks Junos MX Series with service card configured, receipt of a stream of specific packets may crash the MS-PIC component on MS-MIC or MS-MPC. By continuously sending these specific packets, an attacker can repeatedly bring down MS-PIC on MS-MIC/MS-MPC causing a prolonged Denial of Service. This issue affects MX Series devices using MS-PIC, MS-MIC or MS-MPC service cards with any service configured. This issue affects Juniper Networks Junos OS on MX	https://kb.juniper.net/JSA11037	H-JUN-MX80-190820/1413

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Series: 17.2R2-S7; 17.3R3-S4, 17.3R3-S5; 17.4R2-S4 and the subsequent SRs (17.4R2-S5, 17.4R2-S6, etc.); 17.4R3; 18.1R3-S3, 18.1R3-S4, 18.1R3-S5, 18.1R3-S6, 18.1R3-S7, 18.1R3-S8; 18.2R3, 18.2R3-S1, 18.2R3-S2; 18.3R2 and the SRs based on 18.3R2; 18.4R2 and the SRs based on 18.4R2; 19.1R1 and the SRs based on 19.1R1; 19.2R1 and the SRs based on 19.2R1; 19.3R1 and the SRs based on 19.3R1. **CVE ID : CVE-2020-1650**		
Missing Release of Resource after Effective Lifetime	17-Jul-20	3.3	On Juniper Networks MX series, receipt of a stream of specific Layer 2 frames may cause a memory leak resulting in the packet forwarding engine (PFE) on the line card to crash and restart, causing traffic interruption. By continuously sending this stream of specific layer 2 frame, an attacker connected to the same broadcast domain can repeatedly crash the PFE, causing a prolonged Denial of Service (DoS). This issue affects Juniper Networks Junos OS on MX Series: 17.2 versions prior to 17.2R3-S4; 17.2X75 versions prior to 17.2X75-D105.19; 17.3 versions	https://kb.juniper.net/JSA11038	H-JUN-MX80-190820/1414

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			prior to 17.3R3-S7; 17.4 versions prior to 17.4R1-S3, 17.4R2; 18.1 versions prior to 18.1R2. This issue does not affect Juniper Networks Junos OS releases prior to 17.2R1. **CVE ID : CVE-2020-1651**		
Uncontrolled Resource Consumption	17-Jul-20	5	When a device running Juniper Networks Junos OS with MPC7, MPC8, or MPC9 line cards installed and the system is configured for inline IP reassembly, used by L2TP, MAP-E, GRE, and IPIP, the packet forwarding engine (PFE) will become disabled upon receipt of large packets requiring fragmentation, generating the following error messages: [LOG: Err] MQSS(0): WO: Packet Error - Error Packets 1, Connection 29 [LOG: Err] eachip_hmcif_rx_intr_handler(7259): EA[0:0]: HMCIF Rx: Injected checksum error detected on WO response - Chunk Address 0x0 [LOG: Err] MQSS(0): DRD: RORD1: CMD reorder ID error - Command 11, Reorder ID 1838, QID 0 [LOG: Err] MQSS(0): DRD: UNROLL0: HMC chunk length error in stage 5 - Chunk Address: 0x4321f3 [LOG: Err] MQSS(0): DRD: UNROLL0: HMC chunk	https://kb.juniper.net/JSA11041	H-JUN-MX80-190820/1415

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			address error in stage 5 - Chunk Address: 0x0 [LOG: Notice] Error: /fpc/8/pfe/0/cm/0/MQSS(0)/0/MQSS_CMERROR_DRD_RORD_ENG_INT_REG_CMD_FSM_STATE_ERR (0x2203cc), scope: pfe, category: functional, severity: major, module: MQSS(0), type: DRD_RORD_ENG_INT: CMD FSM State Error [LOG: Notice] Performing action cmalarm for error /fpc/8/pfe/0/cm/0/MQSS(0)/0/MQSS_CMERROR_DRD_RORD_ENG_INT_REG_CMD_FSM_STATE_ERR (0x2203cc) in module: MQSS(0) with scope: pfe category: functional level: major [LOG: Notice] Performing action get-state for error /fpc/8/pfe/0/cm/0/MQSS(0)/0/MQSS_CMERROR_DRD_RORD_ENG_INT_REG_CMD_FSM_STATE_ERR (0x2203cc) in module: MQSS(0) with scope: pfe category: functional level: major [LOG: Notice] Performing action disable-pfe for error /fpc/8/pfe/0/cm/0/MQSS(0)/0/MQSS_CMERROR_DRD_RORD_ENG_INT_REG_CMD_FSM_STATE_ERR (0x2203cc) in module: MQSS(0) with scope: pfe		

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			category: functional level: major By continuously sending fragmented packets that cannot be reassembled, an attacker can repeatedly disable the PFE causing a sustained Denial of Service (DoS). This issue affects Juniper Networks Junos OS: 17.2 versions prior to 17.2R3-S4 on MX Series; 17.3 versions prior to 17.3R3-S8 on MX Series; 17.4 versions prior to 17.4R2-S10, 17.4R3-S2 on MX Series; 18.1 versions prior to 18.1R3-S10 on MX Series; 18.2 versions prior to 18.2R3-S3 on MX Series; 18.2X75 versions prior to 18.2X75-D41, 18.2X75-D430, 18.2X75-D65 on MX Series; 18.3 versions prior to 18.3R1-S7, 18.3R2-S4, 18.3R3-S1 on MX Series; 18.4 versions prior to 18.4R1-S7, 18.4R2-S4, 18.4R3 on MX Series; 19.1 versions prior to 19.1R1-S5, 19.1R2-S1, 19.1R3 on MX Series; 19.2 versions prior to 19.2R1-S4, 19.2R2 on MX Series; 19.3 versions prior to 19.3R2-S2, 19.3R3 on MX Series. This issue is specific to inline IP reassembly, introduced in Junos OS 17.2. Versions of Junos OS prior to 17.2 are		

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			unaffected by this vulnerability. **CVE ID : CVE-2020-1655**		
mx960					
Improper Input Validation	17-Jul-20	5	When a device running Juniper Networks Junos OS with MPC7, MPC8, or MPC9 line cards installed and the system is configured for inline IP reassembly, used by L2TP, MAP-E, GRE, and IPIP, the packet forwarding engine (PFE) will become disabled upon receipt of small fragments requiring reassembly, generating the following error messages: [LOG: Err] MQSS(2): WO: Packet Error - Error Packets 1, Connection 29 [LOG: Err] eachip_hmcif_rx_intr_handler(7259): EA[2:0]: HMCIF Rx: Injected checksum error detected on WO response - Chunk Address 0x0 [LOG: Err] MQSS(2): DRD: RORD1: CMD reorder ID error - Command 11, Reorder ID 1960, QID 0 [LOG: Err] MQSS(2): DRD: UNROLL0: HMC chunk address error in stage 5 - Chunk Address: 0xc38fb1 [LOG: Notice] Error: /fpc/0/pfe/0/cm/0/MQSS(2)/2/MQSS_CMERROR_DRD_RORD_ENG_INT_REG_CMD_FSM_STATE_ERR	https://kb.juniper.net/JSA11036	H-JUN-MX96-190820/1416

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			(0x2203cc), scope: pfe, category: functional, severity: major, module: MQSS(2), type: DRD_RORD_ENG_INT: CMD FSM State Error [LOG: Notice] Performing action cmalarm for error /fpc/0/pfe/0/cm/0/MQSS(2)/2/MQSS_CMERROR_DRD_RORD_ENG_INT_REG_CMD_FSM_STATE_ERR (0x2203cc) in module: MQSS(2) with scope: pfe category: functional level: major [LOG: Notice] Performing action get-state for error /fpc/0/pfe/0/cm/0/MQSS(2)/2/MQSS_CMERROR_DRD_RORD_ENG_INT_REG_CMD_FSM_STATE_ERR (0x2203cc) in module: MQSS(2) with scope: pfe category: functional level: major [LOG: Notice] Performing action disable-pfe for error /fpc/0/pfe/0/cm/0/MQSS(2)/2/MQSS_CMERROR_DRD_RORD_ENG_INT_REG_CMD_FSM_STATE_ERR (0x2203cc) in module: MQSS(2) with scope: pfe category: functional level: major By continuously sending fragmented packets that cannot be reassembled, an attacker can repeatedly disable the PFE causing a sustained		

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Denial of Service (DoS). This issue affects Juniper Networks Junos OS: 17.2 versions prior to 17.2R3-S4 on MX Series; 17.3 versions prior to 17.3R3-S8 on MX Series; 17.4 versions prior to 17.4R2-S9, 17.4R3-S1 on MX Series; 18.1 versions prior to 18.1R3-S10 on MX Series; 18.2 versions prior to 18.2R2-S6, 18.2R3-S3 on MX Series; 18.2X75 versions prior to 18.2X75-D34, 18.2X75-D41, 18.2X75-D53, 18.2X75-D65, 18.2X75-D430 on MX Series; 18.3 versions prior to 18.3R1-S7, 18.3R2-S4, 18.3R3-S2 on MX Series; 18.4 versions prior to 18.4R1-S6, 18.4R2-S4, 18.4R3 on MX Series; 19.1 versions prior to 19.1R1-S4, 19.1R2-S1, 19.1R3 on MX Series; 19.2 versions prior to 19.2R1-S3, 19.2R2 on MX Series; 19.3 versions prior to 19.3R2-S2, 19.3R3 on MX Series. This issue is specific to inline IP reassembly, introduced in Junos OS 17.2. Versions of Junos OS prior to 17.2 are unaffected by this vulnerability. **CVE ID : CVE-2020-1649**		
Uncontrolled Resource	17-Jul-20	5	On Juniper Networks Junos MX Series with service	https://kb.juniper.net/JS	H-JUN-MX96-

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Consumption			card configured, receipt of a stream of specific packets may crash the MS-PIC component on MS-MIC or MS-MPC. By continuously sending these specific packets, an attacker can repeatedly bring down MS-PIC on MS-MIC/MS-MPC causing a prolonged Denial of Service. This issue affects MX Series devices using MS-PIC, MS-MIC or MS-MPC service cards with any service configured. This issue affects Juniper Networks Junos OS on MX Series: 17.2R2-S7; 17.3R3-S4, 17.3R3-S5; 17.4R2-S4 and the subsequent SRs (17.4R2-S5, 17.4R2-S6, etc.); 17.4R3; 18.1R3-S3, 18.1R3-S4, 18.1R3-S5, 18.1R3-S6, 18.1R3-S7, 18.1R3-S8; 18.2R3, 18.2R3-S1, 18.2R3-S2; 18.3R2 and the SRs based on 18.3R2; 18.4R2 and the SRs based on 18.4R2; 19.1R1 and the SRs based on 19.1R1; 19.2R1 and the SRs based on 19.2R1; 19.3R1 and the SRs based on 19.3R1. **CVE ID : CVE-2020-1650**	A11037	190820/1417
Missing Release of Resource after Effective	17-Jul-20	3.3	On Juniper Networks MX series, receipt of a stream of specific Layer 2 frames may cause a memory leak resulting in the packet	https://kb.juniper.net/JSA11038	H-JUN-MX96-190820/1418

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Lifetime			forwarding engine (PFE) on the line card to crash and restart, causing traffic interruption. By continuously sending this stream of specific layer 2 frame, an attacker connected to the same broadcast domain can repeatedly crash the PFE, causing a prolonged Denial of Service (DoS). This issue affects Juniper Networks Junos OS on MX Series: 17.2 versions prior to 17.2R3-S4; 17.2X75 versions prior to 17.2X75-D105.19; 17.3 versions prior to 17.3R3-S7; 17.4 versions prior to 17.4R1-S3, 17.4R2; 18.1 versions prior to 18.1R2. This issue does not affect Juniper Networks Junos OS releases prior to 17.2R1. **CVE ID : CVE-2020-1651**		
Uncontrolled Resource Consumption	17-Jul-20	5	When a device running Juniper Networks Junos OS with MPC7, MPC8, or MPC9 line cards installed and the system is configured for inline IP reassembly, used by L2TP, MAP-E, GRE, and IPIP, the packet forwarding engine (PFE) will become disabled upon receipt of large packets requiring fragmentation, generating the following error messages: [LOG: Err]	https://kb.juniper.net/JSA11041	H-JUN-MX96-190820/1419

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			MQSS(0): WO: Packet Error - Error Packets 1, Connection 29 [LOG: Err] eachip_hmcif_rx_intr_handler(7259): EA[0:0]: HMCIF Rx: Injected checksum error detected on WO response - Chunk Address 0x0 [LOG: Err] MQSS(0): DRD: RORD1: CMD reorder ID error - Command 11, Reorder ID 1838, QID 0 [LOG: Err] MQSS(0): DRD: UNROLL0: HMC chunk length error in stage 5 - Chunk Address: 0x4321f3 [LOG: Err] MQSS(0): DRD: UNROLL0: HMC chunk address error in stage 5 - Chunk Address: 0x0 [LOG: Notice] Error: /fpc/8/pfe/0/cm/0/MQSS(0)/0/MQSS_CMERROR_DRD_RORD_ENG_INT_REG_CMD_FSM_STATE_ERR (0x2203cc), scope: pfe, category: functional, severity: major, module: MQSS(0), type: DRD_RORD_ENG_INT: CMD FSM State Error [LOG: Notice] Performing action cmalarm for error /fpc/8/pfe/0/cm/0/MQSS(0)/0/MQSS_CMERROR_DRD_RORD_ENG_INT_REG_CMD_FSM_STATE_ERR (0x2203cc) in module: MQSS(0) with scope: pfe category: functional level: major [LOG: Notice]		

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Performing action get-state for error /fpc/8/pfe/0/cm/0/MQSS(0)/0/MQSS_CMERROR_DRD_RORD_ENG_INT_REG_CMD_FSM_STATE_ERR (0x2203cc) in module: MQSS(0) with scope: pfe category: functional level: major [LOG: Notice] Performing action disable-pfe for error /fpc/8/pfe/0/cm/0/MQSS(0)/0/MQSS_CMERROR_DRD_RORD_ENG_INT_REG_CMD_FSM_STATE_ERR (0x2203cc) in module: MQSS(0) with scope: pfe category: functional level: major By continuously sending fragmented packets that cannot be reassembled, an attacker can repeatedly disable the PFE causing a sustained Denial of Service (DoS). This issue affects Juniper Networks Junos OS: 17.2 versions prior to 17.2R3-S4 on MX Series; 17.3 versions prior to 17.3R3-S8 on MX Series; 17.4 versions prior to 17.4R2-S10, 17.4R3-S2 on MX Series; 18.1 versions prior to 18.1R3-S10 on MX Series; 18.2 versions prior to 18.2R3-S3 on MX Series; 18.2X75 versions prior to 18.2X75-D41, 18.2X75-D430, 18.2X75-D65 on MX		

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Series; 18.3 versions prior to 18.3R1-S7, 18.3R2-S4, 18.3R3-S1 on MX Series; 18.4 versions prior to 18.4R1-S7, 18.4R2-S4, 18.4R3 on MX Series; 19.1 versions prior to 19.1R1-S5, 19.1R2-S1, 19.1R3 on MX Series; 19.2 versions prior to 19.2R1-S4, 19.2R2 on MX Series; 19.3 versions prior to 19.3R2-S2, 19.3R3 on MX Series. This issue is specific to inline IP reassembly, introduced in Junos OS 17.2. Versions of Junos OS prior to 17.2 are unaffected by this vulnerability. **CVE ID : CVE-2020-1655**		
mx10000					
Improper Input Validation	17-Jul-20	5	When a device running Juniper Networks Junos OS with MPC7, MPC8, or MPC9 line cards installed and the system is configured for inline IP reassembly, used by L2TP, MAP-E, GRE, and IPIP, the packet forwarding engine (PFE) will become disabled upon receipt of small fragments requiring reassembly, generating the following error messages: [LOG: Err] MQSS(2): WO: Packet Error - Error Packets 1, Connection 29 [LOG: Err]	https://kb.juniper.net/JSA11036	H-JUN-MX10-190820/1420

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			eachip_hmcif_rx_intr_handler(7259): EA[2:0]: HMCIF Rx: Injected checksum error detected on WO response - Chunk Address 0x0 [LOG: Err] MQSS(2): DRD: RORD1: CMD reorder ID error - Command 11, Reorder ID 1960, QID 0 [LOG: Err] MQSS(2): DRD: UNROLL0: HMC chunk address error in stage 5 - Chunk Address: 0xc38fb1 [LOG: Notice] Error: /fpc/0/pfe/0/cm/0/MQSS(2)/2/MQSS_CMERROR_DRD_RORD_ENG_INT_REG_CMD_FSM_STATE_ERR (0x2203cc), scope: pfe, category: functional, severity: major, module: MQSS(2), type: DRD_RORD_ENG_INT: CMD FSM State Error [LOG: Notice] Performing action cmalarm for error /fpc/0/pfe/0/cm/0/MQSS(2)/2/MQSS_CMERROR_DRD_RORD_ENG_INT_REG_CMD_FSM_STATE_ERR (0x2203cc) in module: MQSS(2) with scope: pfe category: functional level: major [LOG: Notice] Performing action get-state for error /fpc/0/pfe/0/cm/0/MQSS(2)/2/MQSS_CMERROR_DRD_RORD_ENG_INT_REG_CMD_FSM_STATE_ERR (0x2203cc) in module:		

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			MQSS(2) with scope: pfe category: functional level: major [LOG: Notice] Performing action disable-pfe for error /fpc/0/pfe/0/cm/0/MQSS(2)/2/MQSS_CMERROR_DRD_RORD_ENG_INT_REG_CMD_FSM_STATE_ERR (0x2203cc) in module: MQSS(2) with scope: pfe category: functional level: major By continuously sending fragmented packets that cannot be reassembled, an attacker can repeatedly disable the PFE causing a sustained Denial of Service (DoS). This issue affects Juniper Networks Junos OS: 17.2 versions prior to 17.2R3-S4 on MX Series; 17.3 versions prior to 17.3R3-S8 on MX Series; 17.4 versions prior to 17.4R2-S9, 17.4R3-S1 on MX Series; 18.1 versions prior to 18.1R3-S10 on MX Series; 18.2 versions prior to 18.2R2-S6, 18.2R3-S3 on MX Series; 18.2X75 versions prior to 18.2X75-D34, 18.2X75-D41, 18.2X75-D53, 18.2X75-D65, 18.2X75-D430 on MX Series; 18.3 versions prior to 18.3R1-S7, 18.3R2-S4, 18.3R3-S2 on MX Series; 18.4 versions prior to 18.4R1-S6, 18.4R2-S4,		

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			18.4R3 on MX Series; 19.1 versions prior to 19.1R1-S4, 19.1R2-S1, 19.1R3 on MX Series; 19.2 versions prior to 19.2R1-S3, 19.2R2 on MX Series; 19.3 versions prior to 19.3R2-S2, 19.3R3 on MX Series. This issue is specific to inline IP reassembly, introduced in Junos OS 17.2. Versions of Junos OS prior to 17.2 are unaffected by this vulnerability. **CVE ID : CVE-2020-1649**		
Uncontrolled Resource Consumption	17-Jul-20	5	On Juniper Networks Junos MX Series with service card configured, receipt of a stream of specific packets may crash the MS-PIC component on MS-MIC or MS-MPC. By continuously sending these specific packets, an attacker can repeatedly bring down MS-PIC on MS-MIC/MS-MPC causing a prolonged Denial of Service. This issue affects MX Series devices using MS-PIC, MS-MIC or MS-MPC service cards with any service configured. This issue affects Juniper Networks Junos OS on MX Series: 17.2R2-S7; 17.3R3-S4, 17.3R3-S5; 17.4R2-S4 and the subsequent SRs (17.4R2-S5, 17.4R2-S6, etc.); 17.4R3; 18.1R3-S3,	https://kb.juniper.net/JSA11037	H-JUN-MX10-190820/1421

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			18.1R3-S4, 18.1R3-S5, 18.1R3-S6, 18.1R3-S7, 18.1R3-S8; 18.2R3, 18.2R3-S1, 18.2R3-S2; 18.3R2 and the SRs based on 18.3R2; 18.4R2 and the SRs based on 18.4R2; 19.1R1 and the SRs based on 19.1R1; 19.2R1 and the SRs based on 19.2R1; 19.3R1 and the SRs based on 19.3R1. **CVE ID : CVE-2020-1650**		
Missing Release of Resource after Effective Lifetime	17-Jul-20	3.3	On Juniper Networks MX series, receipt of a stream of specific Layer 2 frames may cause a memory leak resulting in the packet forwarding engine (PFE) on the line card to crash and restart, causing traffic interruption. By continuously sending this stream of specific layer 2 frame, an attacker connected to the same broadcast domain can repeatedly crash the PFE, causing a prolonged Denial of Service (DoS). This issue affects Juniper Networks Junos OS on MX Series: 17.2 versions prior to 17.2R3-S4; 17.2X75 versions prior to 17.2X75-D105.19; 17.3 versions prior to 17.3R3-S7; 17.4 versions prior to 17.4R1-S3, 17.4R2; 18.1 versions prior to 18.1R2. This issue does not affect Juniper	https://kb.juniper.net/JSA11038	H-JUN-MX10-190820/1422

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Networks Junos OS releases prior to 17.2R1. **CVE ID : CVE-2020-1651**		
Uncontrolled Resource Consumption	17-Jul-20	5	When a device running Juniper Networks Junos OS with MPC7, MPC8, or MPC9 line cards installed and the system is configured for inline IP reassembly, used by L2TP, MAP-E, GRE, and IPIP, the packet forwarding engine (PFE) will become disabled upon receipt of large packets requiring fragmentation, generating the following error messages: [LOG: Err] MQSS(0): WO: Packet Error - Error Packets 1, Connection 29 [LOG: Err] eachip_hmcif_rx_intr_handler(7259): EA[0:0]: HMCIF Rx: Injected checksum error detected on WO response - Chunk Address 0x0 [LOG: Err] MQSS(0): DRD: RORD1: CMD reorder ID error - Command 11, Reorder ID 1838, QID 0 [LOG: Err] MQSS(0): DRD: UNROLL0: HMC chunk length error in stage 5 - Chunk Address: 0x4321f3 [LOG: Err] MQSS(0): DRD: UNROLL0: HMC chunk address error in stage 5 - Chunk Address: 0x0 [LOG: Notice] Error: /fpc/8/pfe/0/cm/0/MQSS(0)/0/MQSS_CMERROR_D	https://kb.juniper.net/JSA11041	H-JUN-MX10-190820/1423

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			RD_RORD_ENG_INT_REG_CMD_FSM_STATE_ERR (0x2203cc), scope: pfe, category: functional, severity: major, module: MQSS(0), type: DRD_RORD_ENG_INT: CMD FSM State Error [LOG: Notice] Performing action cmalarm for error /fpc/8/pfe/0/cm/0/MQSS(0)/0/MQSS_CMERROR_DRD_RORD_ENG_INT_REG_CMD_FSM_STATE_ERR (0x2203cc) in module: MQSS(0) with scope: pfe category: functional level: major [LOG: Notice] Performing action get-state for error /fpc/8/pfe/0/cm/0/MQSS(0)/0/MQSS_CMERROR_DRD_RORD_ENG_INT_REG_CMD_FSM_STATE_ERR (0x2203cc) in module: MQSS(0) with scope: pfe category: functional level: major [LOG: Notice] Performing action disable-pfe for error /fpc/8/pfe/0/cm/0/MQSS(0)/0/MQSS_CMERROR_DRD_RORD_ENG_INT_REG_CMD_FSM_STATE_ERR (0x2203cc) in module: MQSS(0) with scope: pfe category: functional level: major By continuously sending fragmented packets that cannot be reassembled, an attacker		

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			can repeatedly disable the PFE causing a sustained Denial of Service (DoS). This issue affects Juniper Networks Junos OS: 17.2 versions prior to 17.2R3-S4 on MX Series; 17.3 versions prior to 17.3R3-S8 on MX Series; 17.4 versions prior to 17.4R2-S10, 17.4R3-S2 on MX Series; 18.1 versions prior to 18.1R3-S10 on MX Series; 18.2 versions prior to 18.2R3-S3 on MX Series; 18.2X75 versions prior to 18.2X75-D41, 18.2X75-D430, 18.2X75-D65 on MX Series; 18.3 versions prior to 18.3R1-S7, 18.3R2-S4, 18.3R3-S1 on MX Series; 18.4 versions prior to 18.4R1-S7, 18.4R2-S4, 18.4R3 on MX Series; 19.1 versions prior to 19.1R1-S5, 19.1R2-S1, 19.1R3 on MX Series; 19.2 versions prior to 19.2R1-S4, 19.2R2 on MX Series; 19.3 versions prior to 19.3R2-S2, 19.3R3 on MX Series. This issue is specific to inline IP reassembly, introduced in Junos OS 17.2. Versions of Junos OS prior to 17.2 are unaffected by this vulnerability. **CVE ID : CVE-2020-1655**		
mx10					

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Improper Input Validation	17-Jul-20	5	When a device running Juniper Networks Junos OS with MPC7, MPC8, or MPC9 line cards installed and the system is configured for inline IP reassembly, used by L2TP, MAP-E, GRE, and IPIP, the packet forwarding engine (PFE) will become disabled upon receipt of small fragments requiring reassembly, generating the following error messages: [LOG: Err] MQSS(2): WO: Packet Error - Error Packets 1, Connection 29 [LOG: Err] eachip_hmcif_rx_intr_handler(7259): EA[2:0]: HMCIF Rx: Injected checksum error detected on WO response - Chunk Address 0x0 [LOG: Err] MQSS(2): DRD: RORD1: CMD reorder ID error - Command 11, Reorder ID 1960, QID 0 [LOG: Err] MQSS(2): DRD: UNROLL0: HMC chunk address error in stage 5 - Chunk Address: 0xc38fb1 [LOG: Notice] Error: /fpc/0/pfe/0/cm/0/MQSS(2)/2/MQSS_CMERROR_DRD_RORD_ENG_INT_REG_CMD_FSM_STATE_ERR (0x2203cc), scope: pfe, category: functional, severity: major, module: MQSS(2), type: DRD_RORD_ENG_INT:	https://kb.juniper.net/JSA11036	H-JUN-MX10-190820/1424

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			CMD FSM State Error [LOG: Notice] Performing action cmalarm for error /fpc/0/pfe/0/cm/0/MQSS(2)/2/MQSS_CMERROR_DRD_RORD_ENG_INT_REG_CMD_FSM_STATE_ERR (0x2203cc) in module: MQSS(2) with scope: pfe category: functional level: major [LOG: Notice] Performing action get-state for error /fpc/0/pfe/0/cm/0/MQSS(2)/2/MQSS_CMERROR_DRD_RORD_ENG_INT_REG_CMD_FSM_STATE_ERR (0x2203cc) in module: MQSS(2) with scope: pfe category: functional level: major [LOG: Notice] Performing action disable-pfe for error /fpc/0/pfe/0/cm/0/MQSS(2)/2/MQSS_CMERROR_DRD_RORD_ENG_INT_REG_CMD_FSM_STATE_ERR (0x2203cc) in module: MQSS(2) with scope: pfe category: functional level: major By continuously sending fragmented packets that cannot be reassembled, an attacker can repeatedly disable the PFE causing a sustained Denial of Service (DoS). This issue affects Juniper Networks Junos OS: 17.2 versions prior to 17.2R3-S4 on MX Series; 17.3		

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			versions prior to 17.3R3-S8 on MX Series; 17.4 versions prior to 17.4R2-S9, 17.4R3-S1 on MX Series; 18.1 versions prior to 18.1R3-S10 on MX Series; 18.2 versions prior to 18.2R2-S6, 18.2R3-S3 on MX Series; 18.2X75 versions prior to 18.2X75-D34, 18.2X75-D41, 18.2X75-D53, 18.2X75-D65, 18.2X75-D430 on MX Series; 18.3 versions prior to 18.3R1-S7, 18.3R2-S4, 18.3R3-S2 on MX Series; 18.4 versions prior to 18.4R1-S6, 18.4R2-S4, 18.4R3 on MX Series; 19.1 versions prior to 19.1R1-S4, 19.1R2-S1, 19.1R3 on MX Series; 19.2 versions prior to 19.2R1-S3, 19.2R2 on MX Series; 19.3 versions prior to 19.3R2-S2, 19.3R3 on MX Series. This issue is specific to inline IP reassembly, introduced in Junos OS 17.2. Versions of Junos OS prior to 17.2 are unaffected by this vulnerability. **CVE ID : CVE-2020-1649**		
Uncontrolled Resource Consumption	17-Jul-20	5	On Juniper Networks Junos MX Series with service card configured, receipt of a stream of specific packets may crash the MS-PIC component on MS-MIC or MS-MPC. By	https://kb.juniper.net/JSA11037	H-JUN-MX10-190820/1425

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			continuously sending these specific packets, an attacker can repeatedly bring down MS-PIC on MS-MIC/MS-MPC causing a prolonged Denial of Service. This issue affects MX Series devices using MS-PIC, MS-MIC or MS-MPC service cards with any service configured. This issue affects Juniper Networks Junos OS on MX Series: 17.2R2-S7; 17.3R3-S4, 17.3R3-S5; 17.4R2-S4 and the subsequent SRs (17.4R2-S5, 17.4R2-S6, etc.); 17.4R3; 18.1R3-S3, 18.1R3-S4, 18.1R3-S5, 18.1R3-S6, 18.1R3-S7, 18.1R3-S8; 18.2R3, 18.2R3-S1, 18.2R3-S2; 18.3R2 and the SRs based on 18.3R2; 18.4R2 and the SRs based on 18.4R2; 19.1R1 and the SRs based on 19.1R1; 19.2R1 and the SRs based on 19.2R1; 19.3R1 and the SRs based on 19.3R1. **CVE ID : CVE-2020-1650**		
Missing Release of Resource after Effective Lifetime	17-Jul-20	3.3	On Juniper Networks MX series, receipt of a stream of specific Layer 2 frames may cause a memory leak resulting in the packet forwarding engine (PFE) on the line card to crash and restart, causing traffic interruption. By continuously sending this	https://kb.juniper.net/JSA11038	H-JUN-MX10-190820/1426

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			stream of specific layer 2 frame, an attacker connected to the same broadcast domain can repeatedly crash the PFE, causing a prolonged Denial of Service (DoS). This issue affects Juniper Networks Junos OS on MX Series: 17.2 versions prior to 17.2R3-S4; 17.2X75 versions prior to 17.2X75-D105.19; 17.3 versions prior to 17.3R3-S7; 17.4 versions prior to 17.4R1-S3, 17.4R2; 18.1 versions prior to 18.1R2. This issue does not affect Juniper Networks Junos OS releases prior to 17.2R1. **CVE ID : CVE-2020-1651**		
Uncontrolled Resource Consumption	17-Jul-20	5	When a device running Juniper Networks Junos OS with MPC7, MPC8, or MPC9 line cards installed and the system is configured for inline IP reassembly, used by L2TP, MAP-E, GRE, and IPIP, the packet forwarding engine (PFE) will become disabled upon receipt of large packets requiring fragmentation, generating the following error messages: [LOG: Err] MQSS(0): WO: Packet Error - Error Packets 1, Connection 29 [LOG: Err] eachip_hmcif_rx_intr_handler(7259): EA[0:0]: HMCIF	https://kb.juniper.net/JSA11041	H-JUN-MX10-190820/1427

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Rx: Injected checksum error detected on WO response - Chunk Address 0x0 [LOG: Err] MQSS(0): DRD: RORD1: CMD reorder ID error - Command 11, Reorder ID 1838, QID 0 [LOG: Err] MQSS(0): DRD: UNROLL0: HMC chunk length error in stage 5 - Chunk Address: 0x4321f3 [LOG: Err] MQSS(0): DRD: UNROLL0: HMC chunk address error in stage 5 - Chunk Address: 0x0 [LOG: Notice] Error: /fpc/8/pfe/0/cm/0/MQSS(0)/0/MQSS_CMERROR_DRD_RORD_ENG_INT_REG_CMD_FSM_STATE_ERR (0x2203cc), scope: pfe, category: functional, severity: major, module: MQSS(0), type: DRD_RORD_ENG_INT: CMD FSM State Error [LOG: Notice] Performing action cmalarm for error /fpc/8/pfe/0/cm/0/MQSS(0)/0/MQSS_CMERROR_DRD_RORD_ENG_INT_REG_CMD_FSM_STATE_ERR (0x2203cc) in module: MQSS(0) with scope: pfe category: functional level: major [LOG: Notice] Performing action get-state for error /fpc/8/pfe/0/cm/0/MQSS(0)/0/MQSS_CMERROR_DRD_RORD_ENG_INT_REG_C		

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			MD_FSM_STATE_ERR (0x2203cc) in module: MQSS(0) with scope: pfe category: functional level: major [LOG: Notice] Performing action disable-pfe for error /fpc/8/pfe/0/cm/0/MQSS(0)/0/MQSS_CMERROR_DRD_RORD_ENG_INT_REG_CMD_FSM_STATE_ERR (0x2203cc) in module: MQSS(0) with scope: pfe category: functional level: major By continuously sending fragmented packets that cannot be reassembled, an attacker can repeatedly disable the PFE causing a sustained Denial of Service (DoS). This issue affects Juniper Networks Junos OS: 17.2 versions prior to 17.2R3-S4 on MX Series; 17.3 versions prior to 17.3R3-S8 on MX Series; 17.4 versions prior to 17.4R2-S10, 17.4R3-S2 on MX Series; 18.1 versions prior to 18.1R3-S10 on MX Series; 18.2 versions prior to 18.2R3-S3 on MX Series; 18.2X75 versions prior to 18.2X75-D41, 18.2X75-D430, 18.2X75-D65 on MX Series; 18.3 versions prior to 18.3R1-S7, 18.3R2-S4, 18.3R3-S1 on MX Series; 18.4 versions prior to 18.4R1-S7, 18.4R2-S4,		

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			18.4R3 on MX Series; 19.1 versions prior to 19.1R1-S5, 19.1R2-S1, 19.1R3 on MX Series; 19.2 versions prior to 19.2R1-S4, 19.2R2 on MX Series; 19.3 versions prior to 19.3R2-S2, 19.3R3 on MX Series. This issue is specific to inline IP reassembly, introduced in Junos OS 17.2. Versions of Junos OS prior to 17.2 are unaffected by this vulnerability. **CVE ID : CVE-2020-1655**		
mx10003					
Improper Input Validation	17-Jul-20	5	When a device running Juniper Networks Junos OS with MPC7, MPC8, or MPC9 line cards installed and the system is configured for inline IP reassembly, used by L2TP, MAP-E, GRE, and IPIP, the packet forwarding engine (PFE) will become disabled upon receipt of small fragments requiring reassembly, generating the following error messages: [LOG: Err] MQSS(2): WO: Packet Error - Error Packets 1, Connection 29 [LOG: Err] eachip_hmcif_rx_intr_handler(7259): EA[2:0]: HMCIF Rx: Injected checksum error detected on WO response - Chunk Address	https://kb.juniper.net/JSA11036	H-JUN-MX10-190820/1428

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			0x0 [LOG: Err] MQSS(2): DRD: RORD1: CMD reorder ID error - Command 11, Reorder ID 1960, QID 0 [LOG: Err] MQSS(2): DRD: UNROLL0: HMC chunk address error in stage 5 - Chunk Address: 0xc38fb1 [LOG: Notice] Error: /fpc/0/pfe/0/cm/0/MQSS(2)/2/MQSS_CMERROR_DRD_RORD_ENG_INT_REG_CMD_FSM_STATE_ERR (0x2203cc), scope: pfe, category: functional, severity: major, module: MQSS(2), type: DRD_RORD_ENG_INT: CMD FSM State Error [LOG: Notice] Performing action cmalarm for error /fpc/0/pfe/0/cm/0/MQSS(2)/2/MQSS_CMERROR_DRD_RORD_ENG_INT_REG_CMD_FSM_STATE_ERR (0x2203cc) in module: MQSS(2) with scope: pfe category: functional level: major [LOG: Notice] Performing action get-state for error /fpc/0/pfe/0/cm/0/MQSS(2)/2/MQSS_CMERROR_DRD_RORD_ENG_INT_REG_CMD_FSM_STATE_ERR (0x2203cc) in module: MQSS(2) with scope: pfe category: functional level: major [LOG: Notice] Performing action disable-pfe for error		

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			/fpc/0/pfe/0/cm/0/MQSS(2)/2/MQSS_CMERROR_DRD_RORD_ENG_INT_REG_CMD_FSM_STATE_ERR (0x2203cc) in module: MQSS(2) with scope: pfe category: functional level: major By continuously sending fragmented packets that cannot be reassembled, an attacker can repeatedly disable the PFE causing a sustained Denial of Service (DoS). This issue affects Juniper Networks Junos OS: 17.2 versions prior to 17.2R3-S4 on MX Series; 17.3 versions prior to 17.3R3-S8 on MX Series; 17.4 versions prior to 17.4R2-S9, 17.4R3-S1 on MX Series; 18.1 versions prior to 18.1R3-S10 on MX Series; 18.2 versions prior to 18.2R2-S6, 18.2R3-S3 on MX Series; 18.2X75 versions prior to 18.2X75-D34, 18.2X75-D41, 18.2X75-D53, 18.2X75-D65, 18.2X75-D430 on MX Series; 18.3 versions prior to 18.3R1-S7, 18.3R2-S4, 18.3R3-S2 on MX Series; 18.4 versions prior to 18.4R1-S6, 18.4R2-S4, 18.4R3 on MX Series; 19.1 versions prior to 19.1R1-S4, 19.1R2-S1, 19.1R3 on MX Series; 19.2 versions prior to 19.2R1-S3, 19.2R2		

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			on MX Series; 19.3 versions prior to 19.3R2-S2, 19.3R3 on MX Series. This issue is specific to inline IP reassembly, introduced in Junos OS 17.2. Versions of Junos OS prior to 17.2 are unaffected by this vulnerability. **CVE ID : CVE-2020-1649**		
Uncontrolled Resource Consumption	17-Jul-20	5	On Juniper Networks Junos MX Series with service card configured, receipt of a stream of specific packets may crash the MS-PIC component on MS-MIC or MS-MPC. By continuously sending these specific packets, an attacker can repeatedly bring down MS-PIC on MS-MIC/MS-MPC causing a prolonged Denial of Service. This issue affects MX Series devices using MS-PIC, MS-MIC or MS-MPC service cards with any service configured. This issue affects Juniper Networks Junos OS on MX Series: 17.2R2-S7; 17.3R3-S4, 17.3R3-S5; 17.4R2-S4 and the subsequent SRs (17.4R2-S5, 17.4R2-S6, etc.); 17.4R3; 18.1R3-S3, 18.1R3-S4, 18.1R3-S5, 18.1R3-S6, 18.1R3-S7, 18.1R3-S8; 18.2R3, 18.2R3-S1, 18.2R3-S2; 18.3R2 and the SRs based	https://kb.juniper.net/JSA11037	H-JUN-MX10-190820/1429

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			on 18.3R2; 18.4R2 and the SRs based on 18.4R2; 19.1R1 and the SRs based on 19.1R1; 19.2R1 and the SRs based on 19.2R1; 19.3R1 and the SRs based on 19.3R1. **CVE ID : CVE-2020-1650**		
Missing Release of Resource after Effective Lifetime	17-Jul-20	3.3	On Juniper Networks MX series, receipt of a stream of specific Layer 2 frames may cause a memory leak resulting in the packet forwarding engine (PFE) on the line card to crash and restart, causing traffic interruption. By continuously sending this stream of specific layer 2 frame, an attacker connected to the same broadcast domain can repeatedly crash the PFE, causing a prolonged Denial of Service (DoS). This issue affects Juniper Networks Junos OS on MX Series: 17.2 versions prior to 17.2R3-S4; 17.2X75 versions prior to 17.2X75-D105.19; 17.3 versions prior to 17.3R3-S7; 17.4 versions prior to 17.4R1-S3, 17.4R2; 18.1 versions prior to 18.1R2. This issue does not affect Juniper Networks Junos OS releases prior to 17.2R1. **CVE ID : CVE-2020-1651**	https://kb.juniper.net/JSA11038	H-JUN-MX10-190820/1430
Uncontrolled	17-Jul-20	5	When a device running	https://kb.ju	H-JUN-MX10-

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Resource Consumption			Juniper Networks Junos OS with MPC7, MPC8, or MPC9 line cards installed and the system is configured for inline IP reassembly, used by L2TP, MAP-E, GRE, and IPIP, the packet forwarding engine (PFE) will become disabled upon receipt of large packets requiring fragmentation, generating the following error messages: [LOG: Err] MQSS(0): WO: Packet Error - Error Packets 1, Connection 29 [LOG: Err] eachip_hmcif_rx_intr_handler(7259): EA[0:0]: HMCIF Rx: Injected checksum error detected on WO response - Chunk Address 0x0 [LOG: Err] MQSS(0): DRD: RORD1: CMD reorder ID error - Command 11, Reorder ID 1838, QID 0 [LOG: Err] MQSS(0): DRD: UNROLL0: HMC chunk length error in stage 5 - Chunk Address: 0x4321f3 [LOG: Err] MQSS(0): DRD: UNROLL0: HMC chunk address error in stage 5 - Chunk Address: 0x0 [LOG: Notice] Error: /fpc/8/pfe/0/cm/0/MQSS(0)/0/MQSS_CMERROR_DRD_RORD_ENG_INT_REG_CMD_FSM_STATE_ERR (0x2203cc), scope: pfe, category: functional,	niper.net/JSA11041	190820/1431

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			severity: major, module: MQSS(0), type: DRD_RORD_ENG_INT: CMD FSM State Error [LOG: Notice] Performing action cmalarm for error /fpc/8/pfe/0/cm/0/MQSS(0)/0/MQSS_CMERROR_DRD_RORD_ENG_INT_REG_CMD_FSM_STATE_ERR (0x2203cc) in module: MQSS(0) with scope: pfe category: functional level: major [LOG: Notice] Performing action get-state for error /fpc/8/pfe/0/cm/0/MQSS(0)/0/MQSS_CMERROR_DRD_RORD_ENG_INT_REG_CMD_FSM_STATE_ERR (0x2203cc) in module: MQSS(0) with scope: pfe category: functional level: major [LOG: Notice] Performing action disable-pfe for error /fpc/8/pfe/0/cm/0/MQSS(0)/0/MQSS_CMERROR_DRD_RORD_ENG_INT_REG_CMD_FSM_STATE_ERR (0x2203cc) in module: MQSS(0) with scope: pfe category: functional level: major By continuously sending fragmented packets that cannot be reassembled, an attacker can repeatedly disable the PFE causing a sustained Denial of Service (DoS). This issue affects Juniper		

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Networks Junos OS: 17.2 versions prior to 17.2R3-S4 on MX Series; 17.3 versions prior to 17.3R3-S8 on MX Series; 17.4 versions prior to 17.4R2-S10, 17.4R3-S2 on MX Series; 18.1 versions prior to 18.1R3-S10 on MX Series; 18.2 versions prior to 18.2R3-S3 on MX Series; 18.2X75 versions prior to 18.2X75-D41, 18.2X75-D430, 18.2X75-D65 on MX Series; 18.3 versions prior to 18.3R1-S7, 18.3R2-S4, 18.3R3-S1 on MX Series; 18.4 versions prior to 18.4R1-S7, 18.4R2-S4, 18.4R3 on MX Series; 19.1 versions prior to 19.1R1-S5, 19.1R2-S1, 19.1R3 on MX Series; 19.2 versions prior to 19.2R1-S4, 19.2R2 on MX Series; 19.3 versions prior to 19.3R2-S2, 19.3R3 on MX Series. This issue is specific to inline IP reassembly, introduced in Junos OS 17.2. Versions of Junos OS prior to 17.2 are unaffected by this vulnerability. **CVE ID : CVE-2020-1655**		
mx104					
Improper Input Validation	17-Jul-20	5	When a device running Juniper Networks Junos OS with MPC7, MPC8, or MPC9 line cards installed	https://kb.juniper.net/JSA11036	H-JUN-MX10-190820/1432

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			and the system is configured for inline IP reassembly, used by L2TP, MAP-E, GRE, and IPIP, the packet forwarding engine (PFE) will become disabled upon receipt of small fragments requiring reassembly, generating the following error messages: [LOG: Err] MQSS(2): WO: Packet Error - Error Packets 1, Connection 29 [LOG: Err] eachip_hmcif_rx_intr_handler(7259): EA[2:0]: HMCIF Rx: Injected checksum error detected on WO response - Chunk Address 0x0 [LOG: Err] MQSS(2): DRD: RORD1: CMD reorder ID error - Command 11, Reorder ID 1960, QID 0 [LOG: Err] MQSS(2): DRD: UNROLL0: HMC chunk address error in stage 5 - Chunk Address: 0xc38fb1 [LOG: Notice] Error: /fpc/0/pfe/0/cm/0/MQSS(2)/2/MQSS_CMERROR_DRD_RORD_ENG_INT_REG_CMD_FSM_STATE_ERR (0x2203cc), scope: pfe, category: functional, severity: major, module: MQSS(2), type: DRD_RORD_ENG_INT: CMD FSM State Error [LOG: Notice] Performing action cmalarm for error /fpc/0/pfe/0/cm/0/MQSS		

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			(2)/2/MQSS_CMERROR_DRD_RORD_ENG_INT_REG_CMD_FSM_STATE_ERR (0x2203cc) in module: MQSS(2) with scope: pfe category: functional level: major [LOG: Notice] Performing action get-state for error /fpc/0/pfe/0/cm/0/MQSS(2)/2/MQSS_CMERROR_DRD_RORD_ENG_INT_REG_CMD_FSM_STATE_ERR (0x2203cc) in module: MQSS(2) with scope: pfe category: functional level: major [LOG: Notice] Performing action disable-pfe for error /fpc/0/pfe/0/cm/0/MQSS(2)/2/MQSS_CMERROR_DRD_RORD_ENG_INT_REG_CMD_FSM_STATE_ERR (0x2203cc) in module: MQSS(2) with scope: pfe category: functional level: major By continuously sending fragmented packets that cannot be reassembled, an attacker can repeatedly disable the PFE causing a sustained Denial of Service (DoS). This issue affects Juniper Networks Junos OS: 17.2 versions prior to 17.2R3-S4 on MX Series; 17.3 versions prior to 17.3R3-S8 on MX Series; 17.4 versions prior to 17.4R2-S9, 17.4R3-S1 on MX		

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Series; 18.1 versions prior to 18.1R3-S10 on MX Series; 18.2 versions prior to 18.2R2-S6, 18.2R3-S3 on MX Series; 18.2X75 versions prior to 18.2X75-D34, 18.2X75-D41, 18.2X75-D53, 18.2X75-D65, 18.2X75-D430 on MX Series; 18.3 versions prior to 18.3R1-S7, 18.3R2-S4, 18.3R3-S2 on MX Series; 18.4 versions prior to 18.4R1-S6, 18.4R2-S4, 18.4R3 on MX Series; 19.1 versions prior to 19.1R1-S4, 19.1R2-S1, 19.1R3 on MX Series; 19.2 versions prior to 19.2R1-S3, 19.2R2 on MX Series; 19.3 versions prior to 19.3R2-S2, 19.3R3 on MX Series. This issue is specific to inline IP reassembly, introduced in Junos OS 17.2. Versions of Junos OS prior to 17.2 are unaffected by this vulnerability. **CVE ID : CVE-2020-1649**		
Uncontrolled Resource Consumption	17-Jul-20	5	On Juniper Networks Junos MX Series with service card configured, receipt of a stream of specific packets may crash the MS-PIC component on MS-MIC or MS-MPC. By continuously sending these specific packets, an attacker can repeatedly bring down MS-PIC on MS-	https://kb.juniper.net/JSA11037	H-JUN-MX10-190820/1433

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			MIC/MS-MPC causing a prolonged Denial of Service. This issue affects MX Series devices using MS-PIC, MS-MIC or MS-MPC service cards with any service configured. This issue affects Juniper Networks Junos OS on MX Series: 17.2R2-S7; 17.3R3-S4, 17.3R3-S5; 17.4R2-S4 and the subsequent SRs (17.4R2-S5, 17.4R2-S6, etc.); 17.4R3; 18.1R3-S3, 18.1R3-S4, 18.1R3-S5, 18.1R3-S6, 18.1R3-S7, 18.1R3-S8; 18.2R3, 18.2R3-S1, 18.2R3-S2; 18.3R2 and the SRs based on 18.3R2; 18.4R2 and the SRs based on 18.4R2; 19.1R1 and the SRs based on 19.1R1; 19.2R1 and the SRs based on 19.2R1; 19.3R1 and the SRs based on 19.3R1. **CVE ID : CVE-2020-1650**		
Missing Release of Resource after Effective Lifetime	17-Jul-20	3.3	On Juniper Networks MX series, receipt of a stream of specific Layer 2 frames may cause a memory leak resulting in the packet forwarding engine (PFE) on the line card to crash and restart, causing traffic interruption. By continuously sending this stream of specific layer 2 frame, an attacker connected to the same broadcast domain can	https://kb.juniper.net/JSA11038	H-JUN-MX10-190820/1434

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			repeatedly crash the PFE, causing a prolonged Denial of Service (DoS). This issue affects Juniper Networks Junos OS on MX Series: 17.2 versions prior to 17.2R3-S4; 17.2X75 versions prior to 17.2X75-D105.19; 17.3 versions prior to 17.3R3-S7; 17.4 versions prior to 17.4R1-S3, 17.4R2; 18.1 versions prior to 18.1R2. This issue does not affect Juniper Networks Junos OS releases prior to 17.2R1. **CVE ID : CVE-2020-1651**		
Uncontrolled Resource Consumption	17-Jul-20	5	When a device running Juniper Networks Junos OS with MPC7, MPC8, or MPC9 line cards installed and the system is configured for inline IP reassembly, used by L2TP, MAP-E, GRE, and IPIP, the packet forwarding engine (PFE) will become disabled upon receipt of large packets requiring fragmentation, generating the following error messages: [LOG: Err] MQSS(0): WO: Packet Error - Error Packets 1, Connection 29 [LOG: Err] eachip_hmcif_rx_intr_handler(7259): EA[0:0]: HMCIF Rx: Injected checksum error detected on WO response - Chunk Address 0x0 [LOG: Err] MQSS(0):	https://kb.juniper.net/JSA11041	H-JUN-MX10-190820/1435

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			DRD: RORD1: CMD reorder ID error - Command 11, Reorder ID 1838, QID 0 [LOG: Err] MQSS(0): DRD: UNROLL0: HMC chunk length error in stage 5 - Chunk Address: 0x4321f3 [LOG: Err] MQSS(0): DRD: UNROLL0: HMC chunk address error in stage 5 - Chunk Address: 0x0 [LOG: Notice] Error: /fpc/8/pfe/0/cm/0/MQSS(0)/0/MQSS_CMERROR_DRD_RORD_ENG_INT_REG_CMD_FSM_STATE_ERR (0x2203cc), scope: pfe, category: functional, severity: major, module: MQSS(0), type: DRD_RORD_ENG_INT: CMD FSM State Error [LOG: Notice] Performing action cmalarm for error /fpc/8/pfe/0/cm/0/MQSS(0)/0/MQSS_CMERROR_DRD_RORD_ENG_INT_REG_CMD_FSM_STATE_ERR (0x2203cc) in module: MQSS(0) with scope: pfe category: functional level: major [LOG: Notice] Performing action get-state for error /fpc/8/pfe/0/cm/0/MQSS(0)/0/MQSS_CMERROR_DRD_RORD_ENG_INT_REG_CMD_FSM_STATE_ERR (0x2203cc) in module: MQSS(0) with scope: pfe category: functional level:		

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			major [LOG: Notice] Performing action disable-pfe for error /fpc/8/pfe/0/cm/0/MQSS(0)/0/MQSS_CMERROR_DRD_RORD_ENG_INT_REG_CMD_FSM_STATE_ERR (0x2203cc) in module: MQSS(0) with scope: pfe category: functional level: major By continuously sending fragmented packets that cannot be reassembled, an attacker can repeatedly disable the PFE causing a sustained Denial of Service (DoS). This issue affects Juniper Networks Junos OS: 17.2 versions prior to 17.2R3-S4 on MX Series; 17.3 versions prior to 17.3R3-S8 on MX Series; 17.4 versions prior to 17.4R2-S10, 17.4R3-S2 on MX Series; 18.1 versions prior to 18.1R3-S10 on MX Series; 18.2 versions prior to 18.2R3-S3 on MX Series; 18.2X75 versions prior to 18.2X75-D41, 18.2X75-D430, 18.2X75-D65 on MX Series; 18.3 versions prior to 18.3R1-S7, 18.3R2-S4, 18.3R3-S1 on MX Series; 18.4 versions prior to 18.4R1-S7, 18.4R2-S4, 18.4R3 on MX Series; 19.1 versions prior to 19.1R1-S5, 19.1R2-S1, 19.1R3 on MX Series; 19.2 versions		

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			prior to 19.2R1-S4, 19.2R2 on MX Series; 19.3 versions prior to 19.3R2-S2, 19.3R3 on MX Series. This issue is specific to inline IP reassembly, introduced in Junos OS 17.2. Versions of Junos OS prior to 17.2 are unaffected by this vulnerability. **CVE ID : CVE-2020-1655**		
mx150					
Improper Input Validation	17-Jul-20	5	When a device running Juniper Networks Junos OS with MPC7, MPC8, or MPC9 line cards installed and the system is configured for inline IP reassembly, used by L2TP, MAP-E, GRE, and IPIP, the packet forwarding engine (PFE) will become disabled upon receipt of small fragments requiring reassembly, generating the following error messages: [LOG: Err] MQSS(2): WO: Packet Error - Error Packets 1, Connection 29 [LOG: Err] eachip_hmcif_rx_intr_handler(7259): EA[2:0]: HMCIF Rx: Injected checksum error detected on WO response - Chunk Address 0x0 [LOG: Err] MQSS(2): DRD: RORD1: CMD reorder ID error - Command 11, Reorder ID 1960, QID 0	https://kb.juniper.net/JSA11036	H-JUN-MX15-190820/1436

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			[LOG: Err] MQSS(2): DRD: UNROLL0: HMC chunk address error in stage 5 - Chunk Address: 0xc38fb1 [LOG: Notice] Error: /fpc/0/pfe/0/cm/0/MQSS(2)/2/MQSS_CMERROR_DRD_RORD_ENG_INT_REG_CMD_FSM_STATE_ERR (0x2203cc), scope: pfe, category: functional, severity: major, module: MQSS(2), type: DRD_RORD_ENG_INT: CMD FSM State Error [LOG: Notice] Performing action cmalarm for error /fpc/0/pfe/0/cm/0/MQSS(2)/2/MQSS_CMERROR_DRD_RORD_ENG_INT_REG_CMD_FSM_STATE_ERR (0x2203cc) in module: MQSS(2) with scope: pfe category: functional level: major [LOG: Notice] Performing action get-state for error /fpc/0/pfe/0/cm/0/MQSS(2)/2/MQSS_CMERROR_DRD_RORD_ENG_INT_REG_CMD_FSM_STATE_ERR (0x2203cc) in module: MQSS(2) with scope: pfe category: functional level: major [LOG: Notice] Performing action disable-pfe for error /fpc/0/pfe/0/cm/0/MQSS(2)/2/MQSS_CMERROR_DRD_RORD_ENG_INT_REG_CMD_FSM_STATE_ERR		

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			(0x2203cc) in module: MQSS(2) with scope: pfe category: functional level: major By continuously sending fragmented packets that cannot be reassembled, an attacker can repeatedly disable the PFE causing a sustained Denial of Service (DoS). This issue affects Juniper Networks Junos OS: 17.2 versions prior to 17.2R3-S4 on MX Series; 17.3 versions prior to 17.3R3-S8 on MX Series; 17.4 versions prior to 17.4R2-S9, 17.4R3-S1 on MX Series; 18.1 versions prior to 18.1R3-S10 on MX Series; 18.2 versions prior to 18.2R2-S6, 18.2R3-S3 on MX Series; 18.2X75 versions prior to 18.2X75-D34, 18.2X75-D41, 18.2X75-D53, 18.2X75-D65, 18.2X75-D430 on MX Series; 18.3 versions prior to 18.3R1-S7, 18.3R2-S4, 18.3R3-S2 on MX Series; 18.4 versions prior to 18.4R1-S6, 18.4R2-S4, 18.4R3 on MX Series; 19.1 versions prior to 19.1R1-S4, 19.1R2-S1, 19.1R3 on MX Series; 19.2 versions prior to 19.2R1-S3, 19.2R2 on MX Series; 19.3 versions prior to 19.3R2-S2, 19.3R3 on MX Series. This issue is specific to		

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			inline IP reassembly, introduced in Junos OS 17.2. Versions of Junos OS prior to 17.2 are unaffected by this vulnerability. **CVE ID : CVE-2020-1649**		
Uncontrolled Resource Consumption	17-Jul-20	5	On Juniper Networks Junos MX Series with service card configured, receipt of a stream of specific packets may crash the MS-PIC component on MS-MIC or MS-MPC. By continuously sending these specific packets, an attacker can repeatedly bring down MS-PIC on MS-MIC/MS-MPC causing a prolonged Denial of Service. This issue affects MX Series devices using MS-PIC, MS-MIC or MS-MPC service cards with any service configured. This issue affects Juniper Networks Junos OS on MX Series: 17.2R2-S7; 17.3R3-S4, 17.3R3-S5; 17.4R2-S4 and the subsequent SRs (17.4R2-S5, 17.4R2-S6, etc.); 17.4R3; 18.1R3-S3, 18.1R3-S4, 18.1R3-S5, 18.1R3-S6, 18.1R3-S7, 18.1R3-S8; 18.2R3, 18.2R3-S1, 18.2R3-S2; 18.3R2 and the SRs based on 18.3R2; 18.4R2 and the SRs based on 18.4R2; 19.1R1 and the SRs based on 19.1R1; 19.2R1 and the	https://kb.juniper.net/JSA11037	H-JUN-MX15-190820/1437

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			SRs based on 19.2R1; 19.3R1 and the SRs based on 19.3R1. **CVE ID : CVE-2020-1650**		
Missing Release of Resource after Effective Lifetime	17-Jul-20	3.3	On Juniper Networks MX series, receipt of a stream of specific Layer 2 frames may cause a memory leak resulting in the packet forwarding engine (PFE) on the line card to crash and restart, causing traffic interruption. By continuously sending this stream of specific layer 2 frame, an attacker connected to the same broadcast domain can repeatedly crash the PFE, causing a prolonged Denial of Service (DoS). This issue affects Juniper Networks Junos OS on MX Series: 17.2 versions prior to 17.2R3-S4; 17.2X75 versions prior to 17.2X75-D105.19; 17.3 versions prior to 17.3R3-S7; 17.4 versions prior to 17.4R1-S3, 17.4R2; 18.1 versions prior to 18.1R2. This issue does not affect Juniper Networks Junos OS releases prior to 17.2R1. **CVE ID : CVE-2020-1651**	https://kb.juniper.net/JSA11038	H-JUN-MX15-190820/1438
Uncontrolled Resource Consumption	17-Jul-20	5	When a device running Juniper Networks Junos OS with MPC7, MPC8, or MPC9 line cards installed and the system is	https://kb.juniper.net/JSA11041	H-JUN-MX15-190820/1439

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			configured for inline IP reassembly, used by L2TP, MAP-E, GRE, and IPIP, the packet forwarding engine (PFE) will become disabled upon receipt of large packets requiring fragmentation, generating the following error messages: [LOG: Err] MQSS(0): WO: Packet Error - Error Packets 1, Connection 29 [LOG: Err] eachip_hmcif_rx_intr_handler(7259): EA[0:0]: HMCIF Rx: Injected checksum error detected on WO response - Chunk Address 0x0 [LOG: Err] MQSS(0): DRD: RORD1: CMD reorder ID error - Command 11, Reorder ID 1838, QID 0 [LOG: Err] MQSS(0): DRD: UNROLL0: HMC chunk length error in stage 5 - Chunk Address: 0x4321f3 [LOG: Err] MQSS(0): DRD: UNROLL0: HMC chunk address error in stage 5 - Chunk Address: 0x0 [LOG: Notice] Error: /fpc/8/pfe/0/cm/0/MQSS(0)/0/MQSS_CMERROR_DRD_RORD_ENG_INT_REG_CMD_FSM_STATE_ERR (0x2203cc), scope: pfe, category: functional, severity: major, module: MQSS(0), type: DRD_RORD_ENG_INT: CMD FSM State Error		

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			[LOG: Notice] Performing action cmalarm for error /fpc/8/pfe/0/cm/0/MQSS(0)/0/MQSS_CMERROR_DRD_RORD_ENG_INT_REG_CMD_FSM_STATE_ERR (0x2203cc) in module: MQSS(0) with scope: pfe category: functional level: major [LOG: Notice] Performing action get-state for error /fpc/8/pfe/0/cm/0/MQSS(0)/0/MQSS_CMERROR_DRD_RORD_ENG_INT_REG_CMD_FSM_STATE_ERR (0x2203cc) in module: MQSS(0) with scope: pfe category: functional level: major [LOG: Notice] Performing action disable-pfe for error /fpc/8/pfe/0/cm/0/MQSS(0)/0/MQSS_CMERROR_DRD_RORD_ENG_INT_REG_CMD_FSM_STATE_ERR (0x2203cc) in module: MQSS(0) with scope: pfe category: functional level: major By continuously sending fragmented packets that cannot be reassembled, an attacker can repeatedly disable the PFE causing a sustained Denial of Service (DoS). This issue affects Juniper Networks Junos OS: 17.2 versions prior to 17.2R3-S4 on MX Series; 17.3 versions prior to 17.3R3-		

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			S8 on MX Series; 17.4 versions prior to 17.4R2-S10, 17.4R3-S2 on MX Series; 18.1 versions prior to 18.1R3-S10 on MX Series; 18.2 versions prior to 18.2R3-S3 on MX Series; 18.2X75 versions prior to 18.2X75-D41, 18.2X75-D430, 18.2X75-D65 on MX Series; 18.3 versions prior to 18.3R1-S7, 18.3R2-S4, 18.3R3-S1 on MX Series; 18.4 versions prior to 18.4R1-S7, 18.4R2-S4, 18.4R3 on MX Series; 19.1 versions prior to 19.1R1-S5, 19.1R2-S1, 19.1R3 on MX Series; 19.2 versions prior to 19.2R1-S4, 19.2R2 on MX Series; 19.3 versions prior to 19.3R2-S2, 19.3R3 on MX Series. This issue is specific to inline IP reassembly, introduced in Junos OS 17.2. Versions of Junos OS prior to 17.2 are unaffected by this vulnerability. **CVE ID : CVE-2020-1655**		
mx2008					
Improper Input Validation	17-Jul-20	5	When a device running Juniper Networks Junos OS with MPC7, MPC8, or MPC9 line cards installed and the system is configured for inline IP reassembly, used by L2TP, MAP-E, GRE, and IPIP, the	https://kb.juniper.net/JSA11036	H-JUN-MX20-190820/1440

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			packet forwarding engine (PFE) will become disabled upon receipt of small fragments requiring reassembly, generating the following error messages: [LOG: Err] MQSS(2): WO: Packet Error - Error Packets 1, Connection 29 [LOG: Err] eachip_hmcif_rx_intr_handler(7259): EA[2:0]: HMCIF Rx: Injected checksum error detected on WO response - Chunk Address 0x0 [LOG: Err] MQSS(2): DRD: RORD1: CMD reorder ID error - Command 11, Reorder ID 1960, QID 0 [LOG: Err] MQSS(2): DRD: UNROLL0: HMC chunk address error in stage 5 - Chunk Address: 0xc38fb1 [LOG: Notice] Error: /fpc/0/pfe/0/cm/0/MQSS(2)/2/MQSS_CMERROR_DRD_RORD_ENG_INT_REG_CMD_FSM_STATE_ERR (0x2203cc), scope: pfe, category: functional, severity: major, module: MQSS(2), type: DRD_RORD_ENG_INT: CMD FSM State Error [LOG: Notice] Performing action cmalarm for error /fpc/0/pfe/0/cm/0/MQSS(2)/2/MQSS_CMERROR_DRD_RORD_ENG_INT_REG_CMD_FSM_STATE_ERR (0x2203cc) in module:		

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			MQSS(2) with scope: pfe category: functional level: major [LOG: Notice] Performing action get-state for error /fpc/0/pfe/0/cm/0/MQSS(2)/2/MQSS_CMERROR_DRD_RORD_ENG_INT_REG_CMD_FSM_STATE_ERR (0x2203cc) in module: MQSS(2) with scope: pfe category: functional level: major [LOG: Notice] Performing action disable-pfe for error /fpc/0/pfe/0/cm/0/MQSS(2)/2/MQSS_CMERROR_DRD_RORD_ENG_INT_REG_CMD_FSM_STATE_ERR (0x2203cc) in module: MQSS(2) with scope: pfe category: functional level: major By continuously sending fragmented packets that cannot be reassembled, an attacker can repeatedly disable the PFE causing a sustained Denial of Service (DoS). This issue affects Juniper Networks Junos OS: 17.2 versions prior to 17.2R3-S4 on MX Series; 17.3 versions prior to 17.3R3-S8 on MX Series; 17.4 versions prior to 17.4R2-S9, 17.4R3-S1 on MX Series; 18.1 versions prior to 18.1R3-S10 on MX Series; 18.2 versions prior to 18.2R2-S6, 18.2R3-S3		

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			on MX Series; 18.2X75 versions prior to 18.2X75-D34, 18.2X75-D41, 18.2X75-D53, 18.2X75-D65, 18.2X75-D430 on MX Series; 18.3 versions prior to 18.3R1-S7, 18.3R2-S4, 18.3R3-S2 on MX Series; 18.4 versions prior to 18.4R1-S6, 18.4R2-S4, 18.4R3 on MX Series; 19.1 versions prior to 19.1R1-S4, 19.1R2-S1, 19.1R3 on MX Series; 19.2 versions prior to 19.2R1-S3, 19.2R2 on MX Series; 19.3 versions prior to 19.3R2-S2, 19.3R3 on MX Series. This issue is specific to inline IP reassembly, introduced in Junos OS 17.2. Versions of Junos OS prior to 17.2 are unaffected by this vulnerability. **CVE ID : CVE-2020-1649**		
Uncontrolled Resource Consumption	17-Jul-20	5	On Juniper Networks Junos MX Series with service card configured, receipt of a stream of specific packets may crash the MS-PIC component on MS-MIC or MS-MPC. By continuously sending these specific packets, an attacker can repeatedly bring down MS-PIC on MS-MIC/MS-MPC causing a prolonged Denial of Service. This issue affects MX Series devices using	https://kb.juniper.net/JSA11037	H-JUN-MX20-190820/1441

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			MS-PIC, MS-MIC or MS-MPC service cards with any service configured. This issue affects Juniper Networks Junos OS on MX Series: 17.2R2-S7; 17.3R3-S4, 17.3R3-S5; 17.4R2-S4 and the subsequent SRs (17.4R2-S5, 17.4R2-S6, etc.); 17.4R3; 18.1R3-S3, 18.1R3-S4, 18.1R3-S5, 18.1R3-S6, 18.1R3-S7, 18.1R3-S8; 18.2R3, 18.2R3-S1, 18.2R3-S2; 18.3R2 and the SRs based on 18.3R2; 18.4R2 and the SRs based on 18.4R2; 19.1R1 and the SRs based on 19.1R1; 19.2R1 and the SRs based on 19.2R1; 19.3R1 and the SRs based on 19.3R1. **CVE ID : CVE-2020-1650**		
Missing Release of Resource after Effective Lifetime	17-Jul-20	3.3	On Juniper Networks MX series, receipt of a stream of specific Layer 2 frames may cause a memory leak resulting in the packet forwarding engine (PFE) on the line card to crash and restart, causing traffic interruption. By continuously sending this stream of specific layer 2 frame, an attacker connected to the same broadcast domain can repeatedly crash the PFE, causing a prolonged Denial of Service (DoS). This issue affects Juniper Networks	https://kb.juniper.net/JSA11038	H-JUN-MX20-190820/1442

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Junos OS on MX Series: 17.2 versions prior to 17.2R3-S4; 17.2X75 versions prior to 17.2X75-D105.19; 17.3 versions prior to 17.3R3-S7; 17.4 versions prior to 17.4R1-S3, 17.4R2; 18.1 versions prior to 18.1R2. This issue does not affect Juniper Networks Junos OS releases prior to 17.2R1. **CVE ID : CVE-2020-1651**		
Uncontrolled Resource Consumption	17-Jul-20	5	When a device running Juniper Networks Junos OS with MPC7, MPC8, or MPC9 line cards installed and the system is configured for inline IP reassembly, used by L2TP, MAP-E, GRE, and IPIP, the packet forwarding engine (PFE) will become disabled upon receipt of large packets requiring fragmentation, generating the following error messages: [LOG: Err] MQSS(0): WO: Packet Error - Error Packets 1, Connection 29 [LOG: Err] eachip_hmcif_rx_intr_handler(7259): EA[0:0]: HMCIF Rx: Injected checksum error detected on WO response - Chunk Address 0x0 [LOG: Err] MQSS(0): DRD: RORD1: CMD reorder ID error - Command 11, Reorder ID 1838, QID 0 [LOG: Err] MQSS(0): DRD:	https://kb.juniper.net/JSA11041	H-JUN-MX20-190820/1443

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			UNROLL0: HMC chunk length error in stage 5 - Chunk Address: 0x4321f3 [LOG: Err] MQSS(0): DRD: UNROLL0: HMC chunk address error in stage 5 - Chunk Address: 0x0 [LOG: Notice] Error: /fpc/8/pfe/0/cm/0/MQSS(0)/0/MQSS_CMERROR_DRD_RORD_ENG_INT_REG_CMD_FSM_STATE_ERR (0x2203cc), scope: pfe, category: functional, severity: major, module: MQSS(0), type: DRD_RORD_ENG_INT: CMD FSM State Error [LOG: Notice] Performing action cmalarm for error /fpc/8/pfe/0/cm/0/MQSS(0)/0/MQSS_CMERROR_DRD_RORD_ENG_INT_REG_CMD_FSM_STATE_ERR (0x2203cc) in module: MQSS(0) with scope: pfe category: functional level: major [LOG: Notice] Performing action get-state for error /fpc/8/pfe/0/cm/0/MQSS(0)/0/MQSS_CMERROR_DRD_RORD_ENG_INT_REG_CMD_FSM_STATE_ERR (0x2203cc) in module: MQSS(0) with scope: pfe category: functional level: major [LOG: Notice] Performing action disable-pfe for error /fpc/8/pfe/0/cm/0/MQSS		

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			(0)/0/MQSS_CMERROR_DRD_RORD_ENG_INT_REG_CMD_FSM_STATE_ERR (0x2203cc) in module: MQSS(0) with scope: pfe category: functional level: major By continuously sending fragmented packets that cannot be reassembled, an attacker can repeatedly disable the PFE causing a sustained Denial of Service (DoS). This issue affects Juniper Networks Junos OS: 17.2 versions prior to 17.2R3-S4 on MX Series; 17.3 versions prior to 17.3R3-S8 on MX Series; 17.4 versions prior to 17.4R2-S10, 17.4R3-S2 on MX Series; 18.1 versions prior to 18.1R3-S10 on MX Series; 18.2 versions prior to 18.2R3-S3 on MX Series; 18.2X75 versions prior to 18.2X75-D41, 18.2X75-D430, 18.2X75-D65 on MX Series; 18.3 versions prior to 18.3R1-S7, 18.3R2-S4, 18.3R3-S1 on MX Series; 18.4 versions prior to 18.4R1-S7, 18.4R2-S4, 18.4R3 on MX Series; 19.1 versions prior to 19.1R1-S5, 19.1R2-S1, 19.1R3 on MX Series; 19.2 versions prior to 19.2R1-S4, 19.2R2 on MX Series; 19.3 versions prior to 19.3R2-S2, 19.3R3 on MX Series.		

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			This issue is specific to inline IP reassembly, introduced in Junos OS 17.2. Versions of Junos OS prior to 17.2 are unaffected by this vulnerability. **CVE ID : CVE-2020-1655**		
mx2010					
Improper Input Validation	17-Jul-20	5	When a device running Juniper Networks Junos OS with MPC7, MPC8, or MPC9 line cards installed and the system is configured for inline IP reassembly, used by L2TP, MAP-E, GRE, and IPIP, the packet forwarding engine (PFE) will become disabled upon receipt of small fragments requiring reassembly, generating the following error messages: [LOG: Err] MQSS(2): WO: Packet Error - Error Packets 1, Connection 29 [LOG: Err] eachip_hmcif_rx_intr_handler(7259): EA[2:0]: HMCIF Rx: Injected checksum error detected on WO response - Chunk Address 0x0 [LOG: Err] MQSS(2): DRD: RORD1: CMD reorder ID error - Command 11, Reorder ID 1960, QID 0 [LOG: Err] MQSS(2): DRD: UNROLL0: HMC chunk address error in stage 5 - Chunk Address: 0xc38fb1	https://kb.juniper.net/JSA11036	H-JUN-MX20-190820/1444

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			[LOG: Notice] Error: /fpc/0/pfe/0/cm/0/MQSS(2)/2/MQSS_CMERROR_DRD_RORD_ENG_INT_REG_CMD_FSM_STATE_ERR (0x2203cc), scope: pfe, category: functional, severity: major, module: MQSS(2), type: DRD_RORD_ENG_INT: CMD FSM State Error [LOG: Notice] Performing action cmalarm for error /fpc/0/pfe/0/cm/0/MQSS(2)/2/MQSS_CMERROR_DRD_RORD_ENG_INT_REG_CMD_FSM_STATE_ERR (0x2203cc) in module: MQSS(2) with scope: pfe category: functional level: major [LOG: Notice] Performing action get-state for error /fpc/0/pfe/0/cm/0/MQSS(2)/2/MQSS_CMERROR_DRD_RORD_ENG_INT_REG_CMD_FSM_STATE_ERR (0x2203cc) in module: MQSS(2) with scope: pfe category: functional level: major [LOG: Notice] Performing action disable-pfe for error /fpc/0/pfe/0/cm/0/MQSS(2)/2/MQSS_CMERROR_DRD_RORD_ENG_INT_REG_CMD_FSM_STATE_ERR (0x2203cc) in module: MQSS(2) with scope: pfe category: functional level: major By continuously		

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			sending fragmented packets that cannot be reassembled, an attacker can repeatedly disable the PFE causing a sustained Denial of Service (DoS). This issue affects Juniper Networks Junos OS: 17.2 versions prior to 17.2R3-S4 on MX Series; 17.3 versions prior to 17.3R3-S8 on MX Series; 17.4 versions prior to 17.4R2-S9, 17.4R3-S1 on MX Series; 18.1 versions prior to 18.1R3-S10 on MX Series; 18.2 versions prior to 18.2R2-S6, 18.2R3-S3 on MX Series; 18.2X75 versions prior to 18.2X75-D34, 18.2X75-D41, 18.2X75-D53, 18.2X75-D65, 18.2X75-D430 on MX Series; 18.3 versions prior to 18.3R1-S7, 18.3R2-S4, 18.3R3-S2 on MX Series; 18.4 versions prior to 18.4R1-S6, 18.4R2-S4, 18.4R3 on MX Series; 19.1 versions prior to 19.1R1-S4, 19.1R2-S1, 19.1R3 on MX Series; 19.2 versions prior to 19.2R1-S3, 19.2R2 on MX Series; 19.3 versions prior to 19.3R2-S2, 19.3R3 on MX Series. This issue is specific to inline IP reassembly, introduced in Junos OS 17.2. Versions of Junos OS prior to 17.2 are		

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			unaffected by this vulnerability. **CVE ID : CVE-2020-1649**		
Uncontrolled Resource Consumption	17-Jul-20	5	On Juniper Networks Junos MX Series with service card configured, receipt of a stream of specific packets may crash the MS-PIC component on MS-MIC or MS-MPC. By continuously sending these specific packets, an attacker can repeatedly bring down MS-PIC on MS-MIC/MS-MPC causing a prolonged Denial of Service. This issue affects MX Series devices using MS-PIC, MS-MIC or MS-MPC service cards with any service configured. This issue affects Juniper Networks Junos OS on MX Series: 17.2R2-S7; 17.3R3-S4, 17.3R3-S5; 17.4R2-S4 and the subsequent SRs (17.4R2-S5, 17.4R2-S6, etc.); 17.4R3; 18.1R3-S3, 18.1R3-S4, 18.1R3-S5, 18.1R3-S6, 18.1R3-S7, 18.1R3-S8; 18.2R3, 18.2R3-S1, 18.2R3-S2; 18.3R2 and the SRs based on 18.3R2; 18.4R2 and the SRs based on 18.4R2; 19.1R1 and the SRs based on 19.1R1; 19.2R1 and the SRs based on 19.2R1; 19.3R1 and the SRs based on 19.3R1.	https://kb.juniper.net/JSA11037	H-JUN-MX20-190820/1445

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2020-1650		
Missing Release of Resource after Effective Lifetime	17-Jul-20	3.3	On Juniper Networks MX series, receipt of a stream of specific Layer 2 frames may cause a memory leak resulting in the packet forwarding engine (PFE) on the line card to crash and restart, causing traffic interruption. By continuously sending this stream of specific layer 2 frame, an attacker connected to the same broadcast domain can repeatedly crash the PFE, causing a prolonged Denial of Service (DoS). This issue affects Juniper Networks Junos OS on MX Series: 17.2 versions prior to 17.2R3-S4; 17.2X75 versions prior to 17.2X75-D105.19; 17.3 versions prior to 17.3R3-S7; 17.4 versions prior to 17.4R1-S3, 17.4R2; 18.1 versions prior to 18.1R2. This issue does not affect Juniper Networks Junos OS releases prior to 17.2R1. **CVE ID : CVE-2020-1651**	https://kb.juniper.net/JSA11038	H-JUN-MX20-190820/1446
Uncontrolled Resource Consumption	17-Jul-20	5	When a device running Juniper Networks Junos OS with MPC7, MPC8, or MPC9 line cards installed and the system is configured for inline IP reassembly, used by L2TP, MAP-E, GRE, and IPIP, the	https://kb.juniper.net/JSA11041	H-JUN-MX20-190820/1447

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			packet forwarding engine (PFE) will become disabled upon receipt of large packets requiring fragmentation, generating the following error messages: [LOG: Err] MQSS(0): WO: Packet Error - Error Packets 1, Connection 29 [LOG: Err] eachip_hmcif_rx_intr_handler(7259): EA[0:0]: HMCIF Rx: Injected checksum error detected on WO response - Chunk Address 0x0 [LOG: Err] MQSS(0): DRD: RORD1: CMD reorder ID error - Command 11, Reorder ID 1838, QID 0 [LOG: Err] MQSS(0): DRD: UNROLL0: HMC chunk length error in stage 5 - Chunk Address: 0x4321f3 [LOG: Err] MQSS(0): DRD: UNROLL0: HMC chunk address error in stage 5 - Chunk Address: 0x0 [LOG: Notice] Error: /fpc/8/pfe/0/cm/0/MQSS(0)/0/MQSS_CMERROR_DRD_RORD_ENG_INT_REG_CMD_FSM_STATE_ERR (0x2203cc), scope: pfe, category: functional, severity: major, module: MQSS(0), type: DRD_RORD_ENG_INT: CMD FSM State Error [LOG: Notice] Performing action cmalarm for error /fpc/8/pfe/0/cm/0/MQSS		

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			(0)/0/MQSS_CMERROR_DRD_RORD_ENG_INT_REG_CMD_FSM_STATE_ERR (0x2203cc) in module: MQSS(0) with scope: pfe category: functional level: major [LOG: Notice] Performing action get-state for error /fpc/8/pfe/0/cm/0/MQSS(0)/0/MQSS_CMERROR_DRD_RORD_ENG_INT_REG_CMD_FSM_STATE_ERR (0x2203cc) in module: MQSS(0) with scope: pfe category: functional level: major [LOG: Notice] Performing action disable-pfe for error /fpc/8/pfe/0/cm/0/MQSS(0)/0/MQSS_CMERROR_DRD_RORD_ENG_INT_REG_CMD_FSM_STATE_ERR (0x2203cc) in module: MQSS(0) with scope: pfe category: functional level: major By continuously sending fragmented packets that cannot be reassembled, an attacker can repeatedly disable the PFE causing a sustained Denial of Service (DoS). This issue affects Juniper Networks Junos OS: 17.2 versions prior to 17.2R3-S4 on MX Series; 17.3 versions prior to 17.3R3-S8 on MX Series; 17.4 versions prior to 17.4R2-S10, 17.4R3-S2 on MX		

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Series; 18.1 versions prior to 18.1R3-S10 on MX Series; 18.2 versions prior to 18.2R3-S3 on MX Series; 18.2X75 versions prior to 18.2X75-D41, 18.2X75-D430, 18.2X75-D65 on MX Series; 18.3 versions prior to 18.3R1-S7, 18.3R2-S4, 18.3R3-S1 on MX Series; 18.4 versions prior to 18.4R1-S7, 18.4R2-S4, 18.4R3 on MX Series; 19.1 versions prior to 19.1R1-S5, 19.1R2-S1, 19.1R3 on MX Series; 19.2 versions prior to 19.2R1-S4, 19.2R2 on MX Series; 19.3 versions prior to 19.3R2-S2, 19.3R3 on MX Series. This issue is specific to inline IP reassembly, introduced in Junos OS 17.2. Versions of Junos OS prior to 17.2 are unaffected by this vulnerability. **CVE ID : CVE-2020-1655**		
Netgear					
r6700					
Authentication Bypass by Primary Weakness	28-Jul-20	8.3	This vulnerability allows network-adjacent attackers to bypass authentication on affected installations of NETGEAR R6700 V1.0.4.84_10.0.58 routers. Authentication is not required to exploit this vulnerability. The specific flaw exists within the	N/A	H-NET-R670-190820/1448

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			UPnP service, which listens on TCP port 5000. A crafted UPnP message can be used to bypass authentication. An attacker can leverage this in conjunction with other vulnerabilities to execute arbitrary code in the context of root. Was ZDI-CAN-9642. **CVE ID : CVE-2020-10923**		
Stack-based Buffer Overflow	28-Jul-20	8.3	This vulnerability allows network-adjacent attackers to bypass authentication on affected installations of NETGEAR R6700 V1.0.4.84_10.0.58 routers. Although authentication is required to exploit this vulnerability, the existing authentication mechanism can be bypassed. The specific flaw exists within the UPnP service, which listens on TCP port 5000 by default. The issue results from the lack of proper validation of the length of user-supplied data prior to copying it to a fixed-length, stack-based buffer. An attacker can leverage this vulnerability to execute code in the context of root. Was ZDI-CAN-9643. **CVE ID : CVE-2020-10924**	N/A	H-NET-R670-190820/1449
Improper	28-Jul-20	8.3	This vulnerability allows	N/A	H-NET-R670-

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Certificate Validation			network-adjacent attackers to compromise the integrity of downloaded information on affected installations of NETGEAR R6700 V1.0.4.84_10.0.58 routers. Authentication is not required to exploit this vulnerability. The specific flaw exists within the downloading of files via HTTPS. The issue results from the lack of proper validation of the certificate presented by the server. An attacker can leverage this in conjunction with other vulnerabilities to execute arbitrary code in the context of root. Was ZDI-CAN-9647. **CVE ID : CVE-2020-10925**		190820/1450
Download of Code Without Integrity Check	28-Jul-20	8.3	This vulnerability allows network-adjacent attackers to execute arbitrary code on affected installations of NETGEAR R6700 V1.0.4.84_10.0.58 routers. Authentication is not required to exploit this vulnerability. The specific flaw exists within the handling of firmware updates. The issue results from the lack of proper validation of the firmware image prior to performing an upgrade. An attacker can leverage this in conjunction with other	N/A	H-NET-R670-190820/1451

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			vulnerabilities to execute code in the context of root. Was ZDI-CAN-9648. **CVE ID : CVE-2020-10926**		
Use of a Broken or Risky Cryptographic Algorithm	28-Jul-20	8.3	This vulnerability allows network-adjacent attackers to execute arbitrary code on affected installations of NETGEAR R6700 V1.0.4.84_10.0.58 routers. Authentication is not required to exploit this vulnerability. The specific flaw exists within the encryption of firmware update images. The issue results from the use of an inappropriate encryption algorithm. An attacker can leverage this in conjunction with other vulnerabilities to execute code in the context of root. Was ZDI-CAN-9649. **CVE ID : CVE-2020-10927**	N/A	H-NET-R670-190820/1452
Heap-based Buffer Overflow	28-Jul-20	4.6	This vulnerability allows network-adjacent attackers to execute arbitrary code on affected installations of NETGEAR R6700 V1.0.4.84_10.0.58 routers. Authentication is not required to exploit this vulnerability. The specific flaw exists within the handling of string table file uploads. The issue results from the lack of proper validation of the length of user-supplied data prior to	N/A	H-NET-R670-190820/1453

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			copying it to a fixed-length, heap-based buffer. An attacker can leverage this vulnerability to execute code in the context of the web server. Was ZDI-CAN-9767. **CVE ID : CVE-2020-10928**		
Integer Overflow or Wraparound	28-Jul-20	8.3	This vulnerability allows network-adjacent attackers to execute arbitrary code on affected installations of NETGEAR R6700 V1.0.4.84_10.0.58 routers. Authentication is not required to exploit this vulnerability. The specific flaw exists within the handling of string table file uploads. The issue results from the lack of proper validation of user-supplied data, which can result in an integer overflow before allocating a buffer. An attacker can leverage this vulnerability to execute code in the context of the admin user. Was ZDI-CAN-9768. **CVE ID : CVE-2020-10929**	N/A	H-NET-R670-190820/1454
Improper Access Control	28-Jul-20	3.3	This vulnerability allows network-adjacent attackers to disclose sensitive information on affected installations of NETGEAR R6700 V1.0.4.84_10.0.58 routers. Authentication is not required to exploit this	N/A	H-NET-R670-190820/1455

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			vulnerability. The specific flaw exists within the handling of URLs. The issue results from the lack of proper routing of URLs. An attacker can leverage this vulnerability to disclose stored credentials, leading to further compromise. Was ZDI-CAN-9618. **CVE ID : CVE-2020-10930**		
Stack-based Buffer Overflow	28-Jul-20	8.3	This vulnerability allows network-adjacent attackers to bypass authentication on affected installations of NETGEAR R6700 V1.0.4.84_10.0.58 routers. Authentication is not required to exploit this vulnerability. The specific flaw exists within the httpd service, which listens on TCP port 80 by default. The issue results from the lack of proper validation of the length of user-supplied data prior to copying it to a fixed-length, stack-based buffer. An attacker can leverage this vulnerability to execute code in the context of root. Was ZDI-CAN-9703. **CVE ID : CVE-2020-15416**	N/A	H-NET-R670-190820/1456
Stack-based Buffer Overflow	28-Jul-20	5.8	This vulnerability allows network-adjacent attackers to execute arbitrary code on affected installations of NETGEAR	N/A	H-NET-R670-190820/1457

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			R6700 V1.0.4.84_10.0.58 routers. Authentication is not required to exploit this vulnerability. The specific flaw exists within the handling of string table file uploads. A crafted gui_region in a string table file can trigger an overflow of a fixed-length stack-based buffer. An attacker can leverage this vulnerability to execute code in the context of the web server. Was ZDI-CAN-9756. **CVE ID : CVE-2020-15417**		
Qualcomm					
mdm9206					
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	30-Jul-20	7.5	Possible buffer overflow while parsing mp4 clip with corrupted sample atoms due to improper validation of index in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables in APQ8009, APQ8017, APQ8053, APQ8096AU, APQ8098, Kamorta, MDM9206, MDM9207C, MDM9607, MSM8905, MSM8909W, MSM8917, MSM8920, MSM8937, MSM8940, MSM8953,	https://www.qualcomm.com/company/product-security/bulletins/july-2020-bulletin	H-QUA-MDM9-190820/1458

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			MSM8996, MSM8996AU, MSM8998, Nicobar, QCA6574AU, QCM2150, QCS405, QCS605, QM215, Rennell, SA6155P, Saipan, SDA660, SDA845, SDM429, SDM429W, SDM439, SDM450, SDM630, SDM632, SDM636, SDM660, SDM670, SDM710, SDM845, SDX20, SM6150, SM7150, SM8150, SM8250, SXR1130, SXR2130 **CVE ID : CVE-2020-3688**		
Out-of-bounds Write	30-Jul-20	7.5	Out of bound write while QoS DSCP mapping due to improper input validation for data received from association response frame 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, APQ8098, MDM9150, MDM9206, MDM9207C, MDM9607, MDM9650, MSM8905, MSM8909W, MSM8917, MSM8920, MSM8937, MSM8940, MSM8953, MSM8996AU, Nicobar, QCA6174A, QCA6574AU, QCA9377, QCA9379, QCM2150,	https://www.qualcomm.com/company/product-security/bulletins/july-2020-bulletin	H-QUA-MDM9-190820/1459

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			QCN7605, QCS405, QCS605, QM215, SA6155P, Saipan, SC8180X, SDA845, SDM429, SDM429W, SDM439, SDM450, SDM630, SDM632, SDM636, SDM660, SDM845, SDX20, SDX55, SM8150, SM8250, SXR2130 **CVE ID : CVE-2020-3698**		
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	30-Jul-20	7.5	Possible out of bound access while processing assoc response from host due to improper length check before copying into buffer 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, Nicobar, QCA6174A, QCA6574AU, QCA9377, QCA9379, QCM2150, QCN7605, QCS405, QCS605, QM215, SA6155P, Saipan, SC8180X, SDA845, SDM429, SDM429W,	https://www.qualcomm.com/company/product-security/bulletins/july-2020-bulletin	H-QUA-MDM9-190820/1460

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			SDM439, SDM450, SDM630, SDM632, SDM636, SDM660, SDM845, SDX20, SDX55, SM6150, SM7150, SM8150, SM8250, SXR2130 **CVE ID : CVE-2020-3699**		
mdm9607					
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	30-Jul-20	7.5	Possible buffer overflow while parsing mp4 clip with corrupted sample atoms due to improper validation of index in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables in APQ8009, APQ8017, APQ8053, APQ8096AU, APQ8098, Kamorta, MDM9206, MDM9207C, MDM9607, MSM8905, MSM8909W, MSM8917, MSM8920, MSM8937, MSM8940, MSM8953, MSM8996, MSM8996AU, MSM8998, Nicobar, QCA6574AU, QCM2150, QCS405, QCS605, QM215, Rennell, SA6155P, Saipan, SDA660, SDA845, SDM429, SDM429W, SDM439, SDM450, SDM630, SDM632, SDM636, SDM660, SDM670,	https://www.qualcomm.com/company/product-security/bulletins/july-2020-bulletin	H-QUA-MDM9-190820/1461

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			SDM710, SDM845, SDX20, SM6150, SM7150, SM8150, SM8250, SXR1130, SXR2130 **CVE ID : CVE-2020-3688**		
Out-of-bounds Write	30-Jul-20	7.5	Out of bound write while QoS DSCP mapping due to improper input validation for data received from association response frame 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, APQ8098, MDM9150, MDM9206, MDM9207C, MDM9607, MDM9650, MSM8905, MSM8909W, MSM8917, MSM8920, MSM8937, MSM8940, MSM8953, MSM8996AU, Nicobar, QCA6174A, QCA6574AU, QCA9377, QCA9379, QCM2150, QCN7605, QCS405, QCS605, QM215, SA6155P, Saipan, SC8180X, SDA845, SDM429, SDM429W, SDM439, SDM450, SDM630, SDM632, SDM636, SDM660, SDM845, SDX20, SDX55, SM8150, SM8250,	https://www.qualcomm.com/company/product-security/bulletins/july-2020-bulletin	H-QUA-MDM9-190820/1462

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			SXR2130 **CVE ID : CVE-2020-3698**		
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	30-Jul-20	7.5	Possible out of bound access while processing assoc response from host due to improper length check before copying into buffer 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, Nicobar, QCA6174A, QCA6574AU, QCA9377, QCA9379, QCM2150, QCN7605, QCS405, QCS605, QM215, SA6155P, Saipan, SC8180X, SDA845, SDM429, SDM429W, SDM439, SDM450, SDM630, SDM632, SDM636, SDM660, SDM845, SDX20, SDX55, SM6150, SM7150, SM8150, SM8250, SXR2130 **CVE ID : CVE-2020-3699**	https://www.qualcomm.com/company/product-security/bulletins/july-2020-bulletin	H-QUA-MDM9-190820/1463

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Out-of-bounds Read	30-Jul-20	5	Possible out of bounds read due to a missing bounds check and could lead to local information disclosure in the wifi driver with no additional execution privileges needed in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking in APQ8053, APQ8096AU, IPQ4019, IPQ8064, IPQ8074, MDM9607, MSM8909W, MSM8996AU, QCA6574AU, QCA9531, QCA9558, QCA9980, SC8180X, SDM439, SDX55, SM8150, SM8250, SXR2130 **CVE ID : CVE-2020-3700**	https://www.qualcomm.com/company/product-security/bulletins/july-2020-bulletin	H-QUA-MDM9-190820/1464
msm8909w					
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	30-Jul-20	7.5	Possible buffer overflow while parsing mp4 clip with corrupted sample atoms due to improper validation of index in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music,	https://www.qualcomm.com/company/product-security/bulletins/july-2020-bulletin	H-QUA-MSM8-190820/1465

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Snapdragon Wearables in APQ8009, APQ8017, APQ8053, APQ8096AU, APQ8098, Kamorta, MDM9206, MDM9207C, MDM9607, MSM8905, MSM8909W, MSM8917, MSM8920, MSM8937, MSM8940, MSM8953, MSM8996, MSM8996AU, MSM8998, Nicobar, QCA6574AU, QCM2150, QCS405, QCS605, QM215, Rennell, SA6155P, Saipan, SDA660, SDA845, SDM429, SDM429W, SDM439, SDM450, SDM630, SDM632, SDM636, SDM660, SDM670, SDM710, SDM845, SDX20, SM6150, SM7150, SM8150, SM8250, SXR1130, SXR2130 **CVE ID : CVE-2020-3688**		
Out-of-bounds Write	30-Jul-20	7.5	Out of bound write while QoS DSCP mapping due to improper input validation for data received from association response frame 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, APQ8098, MDM9150,	https://www.qualcomm.com/company/product-security/bulletins/july-2020-bulletin	H-QUA-MSM8-190820/1466

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			MDM9206, MDM9207C, MDM9607, MDM9650, MSM8905, MSM8909W, MSM8917, MSM8920, MSM8937, MSM8940, MSM8953, MSM8996AU, Nicobar, QCA6174A, QCA6574AU, QCA9377, QCA9379, QCM2150, QCN7605, QCS405, QCS605, QM215, SA6155P, Saipan, SC8180X, SDA845, SDM429, SDM429W, SDM439, SDM450, SDM630, SDM632, SDM636, SDM660, SDM845, SDX20, SDX55, SM8150, SM8250, SXR2130 **CVE ID : CVE-2020-3698**		
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	30-Jul-20	7.5	Possible out of bound access while processing assoc response from host due to improper length check before copying into buffer 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,	https://www.qualcomm.com/company/product-security/bulletins/july-2020-bulletin	H-QUA-MSM8-190820/1467

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			MSM8940, MSM8953, MSM8996AU, Nicobar, QCA6174A, QCA6574AU, QCA9377, QCA9379, QCM2150, QCN7605, QCS405, QCS605, QM215, SA6155P, Saipan, SC8180X, SDA845, SDM429, SDM429W, SDM439, SDM450, SDM630, SDM632, SDM636, SDM660, SDM845, SDX20, SDX55, SM6150, SM7150, SM8150, SM8250, SXR2130 **CVE ID : CVE-2020-3699**		
Out-of-bounds Read	30-Jul-20	5	Possible out of bounds read due to a missing bounds check and could lead to local information disclosure in the wifi driver with no additional execution privileges needed in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking in APQ8053, APQ8096AU, IPQ4019, IPQ8064, IPQ8074, MDM9607, MSM8909W, MSM8996AU, QCA6574AU, QCA9531, QCA9558, QCA9980, SC8180X,	https://www.qualcomm.com/company/product-security/bulletins/july-2020-bulletin	H-QUA-MSM8-190820/1468

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			SDM439, SDX55, SM8150, SM8250, SXR2130 **CVE ID : CVE-2020-3700**		
msm8996au					
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	30-Jul-20	7.5	Possible buffer overflow while parsing mp4 clip with corrupted sample atoms due to improper validation of index in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables in APQ8009, APQ8017, APQ8053, APQ8096AU, APQ8098, Kamorta, MDM9206, MDM9207C, MDM9607, MSM8905, MSM8909W, MSM8917, MSM8920, MSM8937, MSM8940, MSM8953, MSM8996, MSM8996AU, MSM8998, Nicobar, QCA6574AU, QCM2150, QCS405, QCS605, QM215, Rennell, SA6155P, Saipan, SDA660, SDA845, SDM429, SDM429W, SDM439, SDM450, SDM630, SDM632, SDM636, SDM660, SDM670, SDM710, SDM845, SDX20, SM6150, SM7150, SM8150, SM8250, SXR1130, SXR2130 **CVE ID : CVE-2020-3688**	https://www.qualcomm.com/company/product-security/bulletins/july-2020-bulletin	H-QUA-MSM8-190820/1469

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Out-of-bounds Write	30-Jul-20	7.5	Out of bound write while QoS DSCP mapping due to improper input validation for data received from association response frame 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, APQ8098, MDM9150, MDM9206, MDM9207C, MDM9607, MDM9650, MSM8905, MSM8909W, MSM8917, MSM8920, MSM8937, MSM8940, MSM8953, MSM8996AU, Nicobar, QCA6174A, QCA6574AU, QCA9377, QCA9379, QCM2150, QCN7605, QCS405, QCS605, QM215, SA6155P, Saipan, SC8180X, SDA845, SDM429, SDM429W, SDM439, SDM450, SDM630, SDM632, SDM636, SDM660, SDM845, SDX20, SDX55, SM8150, SM8250, SXR2130 **CVE ID : CVE-2020-3698**	https://www.qualcomm.com/company/product-security/bulletins/july-2020-bulletin	H-QUA-MSM8-190820/1470
Buffer Copy without Checking Size of Input	30-Jul-20	7.5	Possible out of bound access while processing assoc response from host due to improper length	https://www.qualcomm.com/company/product-	H-QUA-MSM8-190820/1471

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
('Classic Buffer Overflow')			check before copying into buffer 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, Nicobar, QCA6174A, QCA6574AU, QCA9377, QCA9379, QCM2150, QCN7605, QCS405, QCS605, QM215, SA6155P, Saipan, SC8180X, SDA845, SDM429, SDM429W, SDM439, SDM450, SDM630, SDM632, SDM636, SDM660, SDM845, SDX20, SDX55, SM6150, SM7150, SM8150, SM8250, SXR2130 **CVE ID : CVE-2020-3699**	security/bulletins/july-2020-bulletin	
Out-of-bounds Read	30-Jul-20	5	Possible out of bounds read due to a missing bounds check and could lead to local information disclosure in the wifi driver with no additional execution privileges	https://www.qualcomm.com/company/product-security/bulletins/july-2020-	H-QUA-MSM8-190820/1472

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			needed in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking in APQ8053, APQ8096AU, IPQ4019, IPQ8064, IPQ8074, MDM9607, MSM8909W, MSM8996AU, QCA6574AU, QCA9531, QCA9558, QCA9980, SC8180X, SDM439, SDX55, SM8150, SM8250, SXR2130 **CVE ID : CVE-2020-3700**	bulletin	
qca6574au					
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	30-Jul-20	7.5	Possible buffer overflow while parsing mp4 clip with corrupted sample atoms due to improper validation of index in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables in APQ8009, APQ8017, APQ8053, APQ8096AU, APQ8098, Kamorta, MDM9206, MDM9207C, MDM9607, MSM8905, MSM8909W, MSM8917,	https://www.qualcomm.com/company/product-security/bulletins/july-2020-bulletin	H-QUA-QCA6-190820/1473

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			MSM8920, MSM8937, MSM8940, MSM8953, MSM8996, MSM8996AU, MSM8998, Nicobar, QCA6574AU, QCM2150, QCS405, QCS605, QM215, Rennell, SA6155P, Saipan, SDA660, SDA845, SDM429, SDM429W, SDM439, SDM450, SDM630, SDM632, SDM636, SDM660, SDM670, SDM710, SDM845, SDX20, SM6150, SM7150, SM8150, SM8250, SXR1130, SXR2130 **CVE ID : CVE-2020-3688**		
Out-of-bounds Write	30-Jul-20	7.5	Out of bound write while QoS DSCP mapping due to improper input validation for data received from association response frame 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, APQ8098, MDM9150, MDM9206, MDM9207C, MDM9607, MDM9650, MSM8905, MSM8909W, MSM8917, MSM8920, MSM8937, MSM8940, MSM8953, MSM8996AU, Nicobar, QCA6174A,	https://www.qualcomm.com/company/product-security/bulletins/july-2020-bulletin	H-QUA-QCA6-190820/1474

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			QCA6574AU, QCA9377, QCA9379, QCM2150, QCN7605, QCS405, QCS605, QM215, SA6155P, Saipan, SC8180X, SDA845, SDM429, SDM429W, SDM439, SDM450, SDM630, SDM632, SDM636, SDM660, SDM845, SDX20, SDX55, SM8150, SM8250, SXR2130 **CVE ID : CVE-2020-3698**		
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	30-Jul-20	7.5	Possible out of bound access while processing assoc response from host due to improper length check before copying into buffer 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, Nicobar, QCA6174A, QCA6574AU, QCA9377, QCA9379, QCM2150, QCN7605, QCS405, QCS605, QM215, SA6155P, Saipan,	https://www.qualcomm.com/company/product-security/bulletins/july-2020-bulletin	H-QUA-QCA6-190820/1475

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			SC8180X, SDA845, SDM429, SDM429W, SDM439, SDM450, SDM630, SDM632, SDM636, SDM660, SDM845, SDX20, SDX55, SM6150, SM7150, SM8150, SM8250, SXR2130 **CVE ID : CVE-2020-3699**		
Out-of-bounds Read	30-Jul-20	5	Possible out of bounds read due to a missing bounds check and could lead to local information disclosure in the wifi driver with no additional execution privileges needed in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking in APQ8053, APQ8096AU, IPQ4019, IPQ8064, IPQ8074, MDM9607, MSM8909W, MSM8996AU, QCA6574AU, QCA9531, QCA9558, QCA9980, SC8180X, SDM439, SDX55, SM8150, SM8250, SXR2130 **CVE ID : CVE-2020-3700**	https://www.qualcomm.com/company/product-security/bulletins/july-2020-bulletin	H-QUA-QCA6-190820/1476
qcs405					
Use After	30-Jul-20	7.5	Use-after-free issue could occur due to dangling	https://www.qualcomm.	H-QUA-QCS4-

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Free			pointer when generating a frame buffer in OpenGL ES in Snapdragon Compute, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music in APQ8009, Nicobar, QCM2150, QCS405, Saipan, SDM845, SM8150, SM8250, SXR2130 **CVE ID : CVE-2020-3671**	com/company/product-security/bulletins/july-2020-bulletin	190820/1477
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	30-Jul-20	7.5	Possible buffer overflow while parsing mp4 clip with corrupted sample atoms due to improper validation of index in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables in APQ8009, APQ8017, APQ8053, APQ8096AU, APQ8098, Kamorta, MDM9206, MDM9207C, MDM9607, MSM8905, MSM8909W, MSM8917, MSM8920, MSM8937, MSM8940, MSM8953, MSM8996, MSM8996AU, MSM8998, Nicobar, QCA6574AU, QCM2150, QCS405, QCS605, QM215, Rennell, SA6155P, Saipan, SDA660, SDA845, SDM429, SDM429W, SDM439, SDM450, SDM630,	https://www.qualcomm.com/company/product-security/bulletins/july-2020-bulletin	H-QUA-QCS4-190820/1478

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			SDM632, SDM636, SDM660, SDM670, SDM710, SDM845, SDX20, SM6150, SM7150, SM8150, SM8250, SXR1130, SXR2130 **CVE ID : CVE-2020-3688**		
Out-of-bounds Write	30-Jul-20	7.5	Out of bound write while QoS DSCP mapping due to improper input validation for data received from association response frame 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, APQ8098, MDM9150, MDM9206, MDM9207C, MDM9607, MDM9650, MSM8905, MSM8909W, MSM8917, MSM8920, MSM8937, MSM8940, MSM8953, MSM8996AU, Nicobar, QCA6174A, QCA6574AU, QCA9377, QCA9379, QCM2150, QCN7605, QCS405, QCS605, QM215, SA6155P, Saipan, SC8180X, SDA845, SDM429, SDM429W, SDM439, SDM450, SDM630, SDM632, SDM636, SDM660, SDM845, SDX20, SDX55,	https://www.qualcomm.com/company/product-security/bulletins/july-2020-bulletin	H-QUA-QCS4-190820/1479

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			SM8150, SM8250, SXR2130 **CVE ID : CVE-2020-3698**		
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	30-Jul-20	7.5	Possible out of bound access while processing assoc response from host due to improper length check before copying into buffer 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, Nicobar, QCA6174A, QCA6574AU, QCA9377, QCA9379, QCM2150, QCN7605, QCS405, QCS605, QM215, SA6155P, Saipan, SC8180X, SDA845, SDM429, SDM429W, SDM439, SDM450, SDM630, SDM632, SDM636, SDM660, SDM845, SDX20, SDX55, SM6150, SM7150, SM8150, SM8250, SXR2130	https://www.qualcomm.com/company/product-security/bulletins/july-2020-bulletin	H-QUA-QCS4-190820/1480

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2020-3699		
qcs605					
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	30-Jul-20	7.5	Possible buffer overflow while parsing mp4 clip with corrupted sample atoms due to improper validation of index in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables in APQ8009, APQ8017, APQ8053, APQ8096AU, APQ8098, Kamorta, MDM9206, MDM9207C, MDM9607, MSM8905, MSM8909W, MSM8917, MSM8920, MSM8937, MSM8940, MSM8953, MSM8996, MSM8996AU, MSM8998, Nicobar, QCA6574AU, QCM2150, QCS405, QCS605, QM215, Rennell, SA6155P, Saipan, SDA660, SDA845, SDM429, SDM429W, SDM439, SDM450, SDM630, SDM632, SDM636, SDM660, SDM670, SDM710, SDM845, SDX20, SM6150, SM7150, SM8150, SM8250, SXR1130, SXR2130 **CVE ID : CVE-2020-3688**	https://www.qualcomm.com/company/product-security/bulletins/july-2020-bulletin	H-QUA-QCS6-190820/1481
Out-of-bounds	30-Jul-20	7.5	Out of bound write while QoS DSCP mapping due to	https://www.qualcomm.	H-QUA-QCS6-190820/1482

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Write			improper input validation for data received from association response frame 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, APQ8098, MDM9150, MDM9206, MDM9207C, MDM9607, MDM9650, MSM8905, MSM8909W, MSM8917, MSM8920, MSM8937, MSM8940, MSM8953, MSM8996AU, Nicobar, QCA6174A, QCA6574AU, QCA9377, QCA9379, QCM2150, QCN7605, QCS405, QCS605, QM215, SA6155P, Saipan, SC8180X, SDA845, SDM429, SDM429W, SDM439, SDM450, SDM630, SDM632, SDM636, SDM660, SDM845, SDX20, SDX55, SM8150, SM8250, SXR2130 **CVE ID : CVE-2020-3698**	com/company/product-security/bulletins/july-2020-bulletin	
Buffer Copy without Checking Size of Input ('Classic Buffer	30-Jul-20	7.5	Possible out of bound access while processing assoc response from host due to improper length check before copying into buffer in Snapdragon Auto,	https://www.qualcomm.com/company/product-security/bulletins/july-	H-QUA-QCS6-190820/1483

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Overflow')			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, Nicobar, QCA6174A, QCA6574AU, QCA9377, QCA9379, QCM2150, QCN7605, QCS405, QCS605, QM215, SA6155P, Saipan, SC8180X, SDA845, SDM429, SDM429W, SDM439, SDM450, SDM630, SDM632, SDM636, SDM660, SDM845, SDX20, SDX55, SM6150, SM7150, SM8150, SM8250, SXR2130 **CVE ID : CVE-2020-3699**	2020-bulletin	
sda660					
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	30-Jul-20	7.5	Possible buffer overflow while parsing mp4 clip with corrupted sample atoms due to improper validation of index in Snapdragon Auto, Snapdragon Compute,	https://www.qualcomm.com/company/product-security/bulletins/july-2020-	H-QUA-SDA6-190820/1484

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables in APQ8009, APQ8017, APQ8053, APQ8096AU, APQ8098, Kamorta, MDM9206, MDM9207C, MDM9607, MSM8905, MSM8909W, MSM8917, MSM8920, MSM8937, MSM8940, MSM8953, MSM8996, MSM8996AU, MSM8998, Nicobar, QCA6574AU, QCM2150, QCS405, QCS605, QM215, Rennell, SA6155P, Saipan, SDA660, SDA845, SDM429, SDM429W, SDM439, SDM450, SDM630, SDM632, SDM636, SDM660, SDM670, SDM710, SDM845, SDX20, SM6150, SM7150, SM8150, SM8250, SXR1130, SXR2130 **CVE ID : CVE-2020-3688**	bulletin	
sdm439					
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	30-Jul-20	7.5	Possible buffer overflow while parsing mp4 clip with corrupted sample atoms due to improper validation of index in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial	https://www.qualcomm.com/company/product-security/bulletins/july-2020-bulletin	H-QUA-SDM4-190820/1485

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables in APQ8009, APQ8017, APQ8053, APQ8096AU, APQ8098, Kamorta, MDM9206, MDM9207C, MDM9607, MSM8905, MSM8909W, MSM8917, MSM8920, MSM8937, MSM8940, MSM8953, MSM8996, MSM8996AU, MSM8998, Nicobar, QCA6574AU, QCM2150, QCS405, QCS605, QM215, Rennell, SA6155P, Saipan, SDA660, SDA845, SDM429, SDM429W, SDM439, SDM450, SDM630, SDM632, SDM636, SDM660, SDM670, SDM710, SDM845, SDX20, SM6150, SM7150, SM8150, SM8250, SXR1130, SXR2130 **CVE ID : CVE-2020-3688**		
Out-of-bounds Write	30-Jul-20	7.5	Out of bound write while QoS DSCP mapping due to improper input validation for data received from association response frame 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,	https://www.qualcomm.com/company/product-security/bulletins/july-2020-bulletin	H-QUA-SDM4-190820/1486

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			APQ8053, APQ8096AU, APQ8098, MDM9150, MDM9206, MDM9207C, MDM9607, MDM9650, MSM8905, MSM8909W, MSM8917, MSM8920, MSM8937, MSM8940, MSM8953, MSM8996AU, Nicobar, QCA6174A, QCA6574AU, QCA9377, QCA9379, QCM2150, QCN7605, QCS405, QCS605, QM215, SA6155P, Saipan, SC8180X, SDA845, SDM429, SDM429W, SDM439, SDM450, SDM630, SDM632, SDM636, SDM660, SDM845, SDX20, SDX55, SM8150, SM8250, SXR2130 **CVE ID : CVE-2020-3698**		
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	30-Jul-20	7.5	Possible out of bound access while processing assoc response from host due to improper length check before copying into buffer 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,	https://www.qualcomm.com/company/product-security/bulletins/july-2020-bulletin	H-QUA-SDM4-190820/1487

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			MSM8909W, MSM8917, MSM8920, MSM8937, MSM8940, MSM8953, MSM8996AU, Nicobar, QCA6174A, QCA6574AU, QCA9377, QCA9379, QCM2150, QCN7605, QCS405, QCS605, QM215, SA6155P, Saipan, SC8180X, SDA845, SDM429, SDM429W, SDM439, SDM450, SDM630, SDM632, SDM636, SDM660, SDM845, SDX20, SDX55, SM6150, SM7150, SM8150, SM8250, SXR2130 **CVE ID : CVE-2020-3699**		
Out-of-bounds Read	30-Jul-20	5	Possible out of bounds read due to a missing bounds check and could lead to local information disclosure in the wifi driver with no additional execution privileges needed in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking in APQ8053, APQ8096AU, IPQ4019, IPQ8064, IPQ8074, MDM9607, MSM8909W, MSM8996AU, QCA6574AU,	https://www.qualcomm.com/company/product-security/bulletins/july-2020-bulletin	H-QUA-SDM4-190820/1488

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			QCA9531, QCA9558, QCA9980, SC8180X, SDM439, SDX55, SM8150, SM8250, SXR2130 **CVE ID : CVE-2020-3700**		
sdm630					
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	30-Jul-20	7.5	Possible buffer overflow while parsing mp4 clip with corrupted sample atoms due to improper validation of index in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables in APQ8009, APQ8017, APQ8053, APQ8096AU, APQ8098, Kamorta, MDM9206, MDM9207C, MDM9607, MSM8905, MSM8909W, MSM8917, MSM8920, MSM8937, MSM8940, MSM8953, MSM8996, MSM8996AU, MSM8998, Nicobar, QCA6574AU, QCM2150, QCS405, QCS605, QM215, Rennell, SA6155P, Saipan, SDA660, SDA845, SDM429, SDM429W, SDM439, SDM450, SDM630, SDM632, SDM636, SDM660, SDM670, SDM710, SDM845, SDX20, SM6150, SM7150, SM8150, SM8250,	https://www.qualcomm.com/company/product-security/bulletins/july-2020-bulletin	H-QUA-SDM6-190820/1489

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			SXR1130, SXR2130 **CVE ID : CVE-2020-3688**		
Out-of-bounds Write	30-Jul-20	7.5	Out of bound write while QoS DSCP mapping due to improper input validation for data received from association response frame 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, APQ8098, MDM9150, MDM9206, MDM9207C, MDM9607, MDM9650, MSM8905, MSM8909W, MSM8917, MSM8920, MSM8937, MSM8940, MSM8953, MSM8996AU, Nicobar, QCA6174A, QCA6574AU, QCA9377, QCA9379, QCM2150, QCN7605, QCS405, QCS605, QM215, SA6155P, Saipan, SC8180X, SDA845, SDM429, SDM429W, SDM439, SDM450, SDM630, SDM632, SDM636, SDM660, SDM845, SDX20, SDX55, SM8150, SM8250, SXR2130 **CVE ID : CVE-2020-3698**	https://www.qualcomm.com/company/product-security/bulletins/july-2020-bulletin	H-QUA-SDM6-190820/1490
Buffer Copy	30-Jul-20	7.5	Possible out of bound	https://ww	H-QUA-

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
without Checking Size of Input ('Classic Buffer Overflow')			access while processing assoc response from host due to improper length check before copying into buffer 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, Nicobar, QCA6174A, QCA6574AU, QCA9377, QCA9379, QCM2150, QCN7605, QCS405, QCS605, QM215, SA6155P, Saipan, SC8180X, SDA845, SDM429, SDM429W, SDM439, SDM450, SDM630, SDM632, SDM636, SDM660, SDM845, SDX20, SDX55, SM6150, SM7150, SM8150, SM8250, SXR2130 **CVE ID : CVE-2020-3699**	w.qualcomm.com/company/product-security/bulletins/july-2020-bulletin	SDM6-190820/1491
sdm660					
Buffer Copy without	30-Jul-20	7.5	Possible buffer overflow while parsing mp4 clip	https://www.qualcomm.	H-QUA-SDM6-

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Checking Size of Input ('Classic Buffer Overflow')			with corrupted sample atoms due to improper validation of index in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables in APQ8009, APQ8017, APQ8053, APQ8096AU, APQ8098, Kamorta, MDM9206, MDM9207C, MDM9607, MSM8905, MSM8909W, MSM8917, MSM8920, MSM8937, MSM8940, MSM8953, MSM8996, MSM8996AU, MSM8998, Nicobar, QCA6574AU, QCM2150, QCS405, QCS605, QM215, Rennell, SA6155P, Saipan, SDA660, SDA845, SDM429, SDM429W, SDM439, SDM450, SDM630, SDM632, SDM636, SDM660, SDM670, SDM710, SDM845, SDX20, SM6150, SM7150, SM8150, SM8250, SXR1130, SXR2130 **CVE ID : CVE-2020-3688**	com/company/product-security/bulletins/july-2020-bulletin	190820/1492
Out-of-bounds Write	30-Jul-20	7.5	Out of bound write while QoS DSCP mapping due to improper input validation for data received from association response frame in Snapdragon Auto, Snapdragon Compute,	https://www.qualcomm.com/company/product-security/bulletins/july-2020-	H-QUA-SDM6-190820/1493

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables in APQ8009, APQ8017, APQ8053, APQ8096AU, APQ8098, MDM9150, MDM9206, MDM9207C, MDM9607, MDM9650, MSM8905, MSM8909W, MSM8917, MSM8920, MSM8937, MSM8940, MSM8953, MSM8996AU, Nicobar, QCA6174A, QCA6574AU, QCA9377, QCA9379, QCM2150, QCN7605, QCS405, QCS605, QM215, SA6155P, Saipan, SC8180X, SDA845, SDM429, SDM429W, SDM439, SDM450, SDM630, SDM632, SDM636, SDM660, SDM845, SDX20, SDX55, SM8150, SM8250, SXR2130 **CVE ID : CVE-2020-3698**	bulletin	
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	30-Jul-20	7.5	Possible out of bound access while processing assoc response from host due to improper length check before copying into buffer in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial	https://www.qualcomm.com/company/product-security/bulletins/july-2020-bulletin	H-QUA-SDM6-190820/1494

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			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, Nicobar, QCA6174A, QCA6574AU, QCA9377, QCA9379, QCM2150, QCN7605, QCS405, QCS605, QM215, SA6155P, Saipan, SC8180X, SDA845, SDM429, SDM429W, SDM439, SDM450, SDM630, SDM632, SDM636, SDM660, SDM845, SDX20, SDX55, SM6150, SM7150, SM8150, SM8250, SXR2130 **CVE ID : CVE-2020-3699**		
sdx20					
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	30-Jul-20	7.5	Possible buffer overflow while parsing mp4 clip with corrupted sample atoms due to improper validation of index in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music,	https://www.qualcomm.com/company/product-security/bulletins/july-2020-bulletin	H-QUA-SDX2-190820/1495

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Snapdragon Wearables in APQ8009, APQ8017, APQ8053, APQ8096AU, APQ8098, Kamorta, MDM9206, MDM9207C, MDM9607, MSM8905, MSM8909W, MSM8917, MSM8920, MSM8937, MSM8940, MSM8953, MSM8996, MSM8996AU, MSM8998, Nicobar, QCA6574AU, QCM2150, QCS405, QCS605, QM215, Rennell, SA6155P, Saipan, SDA660, SDA845, SDM429, SDM429W, SDM439, SDM450, SDM630, SDM632, SDM636, SDM660, SDM670, SDM710, SDM845, SDX20, SM6150, SM7150, SM8150, SM8250, SXR1130, SXR2130 **CVE ID : CVE-2020-3688**		
Out-of-bounds Write	30-Jul-20	7.5	Out of bound write while QoS DSCP mapping due to improper input validation for data received from association response frame 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, APQ8098, MDM9150,	https://www.qualcomm.com/company/product-security/bulletins/july-2020-bulletin	H-QUA-SDX2-190820/1496

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			MDM9206, MDM9207C, MDM9607, MDM9650, MSM8905, MSM8909W, MSM8917, MSM8920, MSM8937, MSM8940, MSM8953, MSM8996AU, Nicobar, QCA6174A, QCA6574AU, QCA9377, QCA9379, QCM2150, QCN7605, QCS405, QCS605, QM215, SA6155P, Saipan, SC8180X, SDA845, SDM429, SDM429W, SDM439, SDM450, SDM630, SDM632, SDM636, SDM660, SDM845, SDX20, SDX55, SM8150, SM8250, SXR2130 **CVE ID : CVE-2020-3698**		
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	30-Jul-20	7.5	Possible out of bound access while processing assoc response from host due to improper length check before copying into buffer 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,	https://www.qualcomm.com/company/product-security/bulletins/july-2020-bulletin	H-QUA-SDX2-190820/1497

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			MSM8940, MSM8953, MSM8996AU, Nicobar, QCA6174A, QCA6574AU, QCA9377, QCA9379, QCM2150, QCN7605, QCS405, QCS605, QM215, SA6155P, Saipan, SC8180X, SDA845, SDM429, SDM429W, SDM439, SDM450, SDM630, SDM632, SDM636, SDM660, SDM845, SDX20, SDX55, SM6150, SM7150, SM8150, SM8250, SXR2130 **CVE ID : CVE-2020-3699**		
mdm9150					
Out-of-bounds Write	30-Jul-20	7.5	Out of bound write while QoS DSCP mapping due to improper input validation for data received from association response frame 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, APQ8098, MDM9150, MDM9206, MDM9207C, MDM9607, MDM9650, MSM8905, MSM8909W, MSM8917, MSM8920, MSM8937, MSM8940,	https://www.qualcomm.com/company/product-security/bulletins/july-2020-bulletin	H-QUA-MDM9-190820/1498

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			MSM8953, MSM8996AU, Nicobar, QCA6174A, QCA6574AU, QCA9377, QCA9379, QCM2150, QCN7605, QCS405, QCS605, QM215, SA6155P, Saipan, SC8180X, SDA845, SDM429, SDM429W, SDM439, SDM450, SDM630, SDM632, SDM636, SDM660, SDM845, SDX20, SDX55, SM8150, SM8250, SXR2130 **CVE ID : CVE-2020-3698**		
mdm9640					
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	30-Jul-20	7.5	Possible out of bound access while processing assoc response from host due to improper length check before copying into buffer 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, Nicobar, QCA6174A, QCA6574AU,	https://www.qualcomm.com/company/product-security/bulletins/july-2020-bulletin	H-QUA-MDM9-190820/1499

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			QCA9377, QCA9379, QCM2150, QCN7605, QCS405, QCS605, QM215, SA6155P, Saipan, SC8180X, SDA845, SDM429, SDM429W, SDM439, SDM450, SDM630, SDM632, SDM636, SDM660, SDM845, SDX20, SDX55, SM6150, SM7150, SM8150, SM8250, SXR2130 **CVE ID : CVE-2020-3699**		
mdm9650					
Out-of-bounds Write	30-Jul-20	7.5	Out of bound write while QoS DSCP mapping due to improper input validation for data received from association response frame 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, APQ8098, MDM9150, MDM9206, MDM9207C, MDM9607, MDM9650, MSM8905, MSM8909W, MSM8917, MSM8920, MSM8937, MSM8940, MSM8953, MSM8996AU, Nicobar, QCA6174A, QCA6574AU, QCA9377,	https://www.qualcomm.com/company/product-security/bulletins/july-2020-bulletin	H-QUA-MDM9-190820/1500

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			QCA9379, QCM2150, QCN7605, QCS405, QCS605, QM215, SA6155P, Saipan, SC8180X, SDA845, SDM429, SDM429W, SDM439, SDM450, SDM630, SDM632, SDM636, SDM660, SDM845, SDX20, SDX55, SM8150, SM8250, SXR2130 **CVE ID : CVE-2020-3698**		
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	30-Jul-20	7.5	Possible out of bound access while processing assoc response from host due to improper length check before copying into buffer 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, Nicobar, QCA6174A, QCA6574AU, QCA9377, QCA9379, QCM2150, QCN7605, QCS405, QCS605, QM215, SA6155P, Saipan, SC8180X, SDA845,	https://www.qualcomm.com/company/product-security/bulletins/july-2020-bulletin	H-QUA-MDM9-190820/1501

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			SDM429, SDM429W, SDM439, SDM450, SDM630, SDM632, SDM636, SDM660, SDM845, SDX20, SDX55, SM6150, SM7150, SM8150, SM8250, SXR2130 **CVE ID : CVE-2020-3699**		
ipq4019					
Out-of-bounds Read	30-Jul-20	5	Possible out of bounds read due to a missing bounds check and could lead to local information disclosure in the wifi driver with no additional execution privileges needed in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking in APQ8053, APQ8096AU, IPQ4019, IPQ8064, IPQ8074, MDM9607, MSM8909W, MSM8996AU, QCA6574AU, QCA9531, QCA9558, QCA9980, SC8180X, SDM439, SDX55, SM8150, SM8250, SXR2130 **CVE ID : CVE-2020-3700**	https://www.qualcomm.com/company/product-security/bulletins/july-2020-bulletin	H-QUA-IPQ4-190820/1502
ipq8064					
Out-of-	30-Jul-20	5	Possible out of bounds	https://ww	H-QUA-IPQ8-

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
bounds Read			read due to a missing bounds check and could lead to local information disclosure in the wifi driver with no additional execution privileges needed in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking in APQ8053, APQ8096AU, IPQ4019, IPQ8064, IPQ8074, MDM9607, MSM8909W, MSM8996AU, QCA6574AU, QCA9531, QCA9558, QCA9980, SC8180X, SDM439, SDX55, SM8150, SM8250, SXR2130 **CVE ID : CVE-2020-3700**	w.qualcomm.com/company/product-security/bulletins/july-2020-bulletin	190820/1503
ipq8074					
Out-of-bounds Read	30-Jul-20	5	Possible out of bounds read due to a missing bounds check and could lead to local information disclosure in the wifi driver with no additional execution privileges needed in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Mobile,	https://www.qualcomm.com/company/product-security/bulletins/july-2020-bulletin	H-QUA-IPQ8-190820/1504

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking in APQ8053, APQ8096AU, IPQ4019, IPQ8064, IPQ8074, MDM9607, MSM8909W, MSM8996AU, QCA6574AU, QCA9531, QCA9558, QCA9980, SC8180X, SDM439, SDX55, SM8150, SM8250, SXR2130 **CVE ID : CVE-2020-3700**		
qca6174a					
Out-of-bounds Write	30-Jul-20	7.5	Out of bound write while QoS DSCP mapping due to improper input validation for data received from association response frame 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, APQ8098, MDM9150, MDM9206, MDM9207C, MDM9607, MDM9650, MSM8905, MSM8909W, MSM8917, MSM8920, MSM8937, MSM8940, MSM8953, MSM8996AU, Nicobar, QCA6174A, QCA6574AU, QCA9377,	https://www.qualcomm.com/company/product-security/bulletins/july-2020-bulletin	H-QUA-QCA6-190820/1505

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			QCA9379, QCM2150, QCN7605, QCS405, QCS605, QM215, SA6155P, Saipan, SC8180X, SDA845, SDM429, SDM429W, SDM439, SDM450, SDM630, SDM632, SDM636, SDM660, SDM845, SDX20, SDX55, SM8150, SM8250, SXR2130 **CVE ID : CVE-2020-3698**		
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	30-Jul-20	7.5	Possible out of bound access while processing assoc response from host due to improper length check before copying into buffer 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, Nicobar, QCA6174A, QCA6574AU, QCA9377, QCA9379, QCM2150, QCN7605, QCS405, QCS605, QM215, SA6155P, Saipan, SC8180X, SDA845,	https://www.qualcomm.com/company/product-security/bulletins/july-2020-bulletin	H-QUA-QCA6-190820/1506

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			SDM429, SDM429W, SDM439, SDM450, SDM630, SDM632, SDM636, SDM660, SDM845, SDX20, SDX55, SM6150, SM7150, SM8150, SM8250, SXR2130 **CVE ID : CVE-2020-3699**		
qca9377					
Out-of-bounds Write	30-Jul-20	7.5	Out of bound write while QoS DSCP mapping due to improper input validation for data received from association response frame 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, APQ8098, MDM9150, MDM9206, MDM9207C, MDM9607, MDM9650, MSM8905, MSM8909W, MSM8917, MSM8920, MSM8937, MSM8940, MSM8953, MSM8996AU, Nicobar, QCA6174A, QCA6574AU, QCA9377, QCA9379, QCM2150, QCN7605, QCS405, QCS605, QM215, SA6155P, Saipan, SC8180X, SDA845, SDM429, SDM429W,	https://www.qualcomm.com/company/product-security/bulletins/july-2020-bulletin	H-QUA-QCA9-190820/1507

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			SDM439, SDM450, SDM630, SDM632, SDM636, SDM660, SDM845, SDX20, SDX55, SM8150, SM8250, SXR2130 **CVE ID : CVE-2020-3698**		
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	30-Jul-20	7.5	Possible out of bound access while processing assoc response from host due to improper length check before copying into buffer 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, Nicobar, QCA6174A, QCA6574AU, QCA9377, QCA9379, QCM2150, QCN7605, QCS405, QCS605, QM215, SA6155P, Saipan, SC8180X, SDA845, SDM429, SDM429W, SDM439, SDM450, SDM630, SDM632, SDM636, SDM660, SDM845, SDX20, SDX55,	https://www.qualcomm.com/company/product-security/bulletins/july-2020-bulletin	H-QUA-QCA9-190820/1508

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			SM6150, SM7150, SM8150, SM8250, SXR2130 **CVE ID : CVE-2020-3699**		
qca9379					
Out-of-bounds Write	30-Jul-20	7.5	Out of bound write while QoS DSCP mapping due to improper input validation for data received from association response frame 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, APQ8098, MDM9150, MDM9206, MDM9207C, MDM9607, MDM9650, MSM8905, MSM8909W, MSM8917, MSM8920, MSM8937, MSM8940, MSM8953, MSM8996AU, Nicobar, QCA6174A, QCA6574AU, QCA9377, QCA9379, QCM2150, QCN7605, QCS405, QCS605, QM215, SA6155P, Saipan, SC8180X, SDA845, SDM429, SDM429W, SDM439, SDM450, SDM630, SDM632, SDM636, SDM660, SDM845, SDX20, SDX55, SM8150, SM8250,	https://www.qualcomm.com/company/product-security/bulletins/july-2020-bulletin	H-QUA-QCA9-190820/1509

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			SXR2130 **CVE ID : CVE-2020-3698**		
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	30-Jul-20	7.5	Possible out of bound access while processing assoc response from host due to improper length check before copying into buffer 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, Nicobar, QCA6174A, QCA6574AU, QCA9377, QCA9379, QCM2150, QCN7605, QCS405, QCS605, QM215, SA6155P, Saipan, SC8180X, SDA845, SDM429, SDM429W, SDM439, SDM450, SDM630, SDM632, SDM636, SDM660, SDM845, SDX20, SDX55, SM6150, SM7150, SM8150, SM8250, SXR2130 **CVE ID : CVE-2020-3699**	https://www.qualcomm.com/company/product-security/bulletins/july-2020-bulletin	H-QUA-QCA9-190820/1510

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
sdm429w					
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	30-Jul-20	7.5	Possible buffer overflow while parsing mp4 clip with corrupted sample atoms due to improper validation of index in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables in APQ8009, APQ8017, APQ8053, APQ8096AU, APQ8098, Kamorta, MDM9206, MDM9207C, MDM9607, MSM8905, MSM8909W, MSM8917, MSM8920, MSM8937, MSM8940, MSM8953, MSM8996, MSM8996AU, MSM8998, Nicobar, QCA6574AU, QCM2150, QCS405, QCS605, QM215, Rennell, SA6155P, Saipan, SDA660, SDA845, SDM429, SDM429W, SDM439, SDM450, SDM630, SDM632, SDM636, SDM660, SDM670, SDM710, SDM845, SDX20, SM6150, SM7150, SM8150, SM8250, SXR1130, SXR2130 **CVE ID : CVE-2020-3688**	https://www.qualcomm.com/company/product-security/bulletins/july-2020-bulletin	H-QUA-SDM4-190820/1511
Out-of-bounds Write	30-Jul-20	7.5	Out of bound write while QoS DSCP mapping due to improper input validation	https://www.qualcomm.com/compan	H-QUA-SDM4-190820/1512

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			for data received from association response frame 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, APQ8098, MDM9150, MDM9206, MDM9207C, MDM9607, MDM9650, MSM8905, MSM8909W, MSM8917, MSM8920, MSM8937, MSM8940, MSM8953, MSM8996AU, Nicobar, QCA6174A, QCA6574AU, QCA9377, QCA9379, QCM2150, QCN7605, QCS405, QCS605, QM215, SA6155P, Saipan, SC8180X, SDA845, SDM429, SDM429W, SDM439, SDM450, SDM630, SDM632, SDM636, SDM660, SDM845, SDX20, SDX55, SM8150, SM8250, SXR2130 **CVE ID : CVE-2020-3698**	y/product-security/bulletins/july-2020-bulletin	
Buffer Copy without Checking Size of Input ('Classic Buffer	30-Jul-20	7.5	Possible out of bound access while processing assoc response from host due to improper length check before copying into buffer in Snapdragon Auto, Snapdragon Compute,	https://www.qualcomm.com/company/product-security/bulletins/july-2020-	H-QUA-SDM4-190820/1513

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Overflow')			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, Nicobar, QCA6174A, QCA6574AU, QCA9377, QCA9379, QCM2150, QCN7605, QCS405, QCS605, QM215, SA6155P, Saipan, SC8180X, SDA845, SDM429, SDM429W, SDM439, SDM450, SDM630, SDM632, SDM636, SDM660, SDM845, SDX20, SDX55, SM6150, SM7150, SM8150, SM8250, SXR2130 **CVE ID : CVE-2020-3699**	bulletin	
apq8009					
Use After Free	30-Jul-20	7.5	Use-after-free issue could occur due to dangling pointer when generating a frame buffer in OpenGL ES in Snapdragon Compute, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile,	https://www.qualcomm.com/company/product-security/bulletins/july-2020-bulletin	H-QUA-APQ8-190820/1514

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Snapdragon Voice & Music in APQ8009, Nicobar, QCM2150, QCS405, Saipan, SDM845, SM8150, SM8250, SXR2130 **CVE ID : CVE-2020-3671**		
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	30-Jul-20	7.5	Possible buffer overflow while parsing mp4 clip with corrupted sample atoms due to improper validation of index in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables in APQ8009, APQ8017, APQ8053, APQ8096AU, APQ8098, Kamorta, MDM9206, MDM9207C, MDM9607, MSM8905, MSM8909W, MSM8917, MSM8920, MSM8937, MSM8940, MSM8953, MSM8996, MSM8996AU, MSM8998, Nicobar, QCA6574AU, QCM2150, QCS405, QCS605, QM215, Rennell, SA6155P, Saipan, SDA660, SDA845, SDM429, SDM429W, SDM439, SDM450, SDM630, SDM632, SDM636, SDM660, SDM670, SDM710, SDM845, SDX20, SM6150, SM7150, SM8150, SM8250,	https://www.qualcomm.com/company/product-security/bulletins/july-2020-bulletin	H-QUA-APQ8-190820/1515

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			SXR1130, SXR2130 **CVE ID : CVE-2020-3688**		
Out-of-bounds Write	30-Jul-20	7.5	Out of bound write while QoS DSCP mapping due to improper input validation for data received from association response frame 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, APQ8098, MDM9150, MDM9206, MDM9207C, MDM9607, MDM9650, MSM8905, MSM8909W, MSM8917, MSM8920, MSM8937, MSM8940, MSM8953, MSM8996AU, Nicobar, QCA6174A, QCA6574AU, QCA9377, QCA9379, QCM2150, QCN7605, QCS405, QCS605, QM215, SA6155P, Saipan, SC8180X, SDA845, SDM429, SDM429W, SDM439, SDM450, SDM630, SDM632, SDM636, SDM660, SDM845, SDX20, SDX55, SM8150, SM8250, SXR2130 **CVE ID : CVE-2020-3698**	https://www.qualcomm.com/company/product-security/bulletins/july-2020-bulletin	H-QUA-APQ8-190820/1516
Buffer Copy	30-Jul-20	7.5	Possible out of bound	https://ww	H-QUA-APQ8-

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
without Checking Size of Input ('Classic Buffer Overflow')			access while processing assoc response from host due to improper length check before copying into buffer 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, Nicobar, QCA6174A, QCA6574AU, QCA9377, QCA9379, QCM2150, QCN7605, QCS405, QCS605, QM215, SA6155P, Saipan, SC8180X, SDA845, SDM429, SDM429W, SDM439, SDM450, SDM630, SDM632, SDM636, SDM660, SDM845, SDX20, SDX55, SM6150, SM7150, SM8150, SM8250, SXR2130 **CVE ID : CVE-2020-3699**	w.qualcomm.com/company/product-security/bulletins/july-2020-bulletin	190820/1517
apq8098					
Buffer Copy without	30-Jul-20	7.5	Possible buffer overflow while parsing mp4 clip	https://www.qualcomm.	H-QUA-APQ8-190820/1518

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Checking Size of Input ('Classic Buffer Overflow')			with corrupted sample atoms due to improper validation of index in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables in APQ8009, APQ8017, APQ8053, APQ8096AU, APQ8098, Kamorta, MDM9206, MDM9207C, MDM9607, MSM8905, MSM8909W, MSM8917, MSM8920, MSM8937, MSM8940, MSM8953, MSM8996, MSM8996AU, MSM8998, Nicobar, QCA6574AU, QCM2150, QCS405, QCS605, QM215, Rennell, SA6155P, Saipan, SDA660, SDA845, SDM429, SDM429W, SDM439, SDM450, SDM630, SDM632, SDM636, SDM660, SDM670, SDM710, SDM845, SDX20, SM6150, SM7150, SM8150, SM8250, SXR1130, SXR2130 **CVE ID : CVE-2020-3688**	com/company/product-security/bulletins/july-2020-bulletin	
Out-of-bounds Write	30-Jul-20	7.5	Out of bound write while QoS DSCP mapping due to improper input validation for data received from association response frame in Snapdragon Auto, Snapdragon Compute,	https://www.qualcomm.com/company/product-security/bulletins/july-2020-	H-QUA-APQ8-190820/1519

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables in APQ8009, APQ8017, APQ8053, APQ8096AU, APQ8098, MDM9150, MDM9206, MDM9207C, MDM9607, MDM9650, MSM8905, MSM8909W, MSM8917, MSM8920, MSM8937, MSM8940, MSM8953, MSM8996AU, Nicobar, QCA6174A, QCA6574AU, QCA9377, QCA9379, QCM2150, QCN7605, QCS405, QCS605, QM215, SA6155P, Saipan, SC8180X, SDA845, SDM429, SDM429W, SDM439, SDM450, SDM630, SDM632, SDM636, SDM660, SDM845, SDX20, SDX55, SM8150, SM8250, SXR2130 **CVE ID : CVE-2020-3698**	bulletin	
msm8953					
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	30-Jul-20	7.5	Possible buffer overflow while parsing mp4 clip with corrupted sample atoms due to improper validation of index in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer	https://www.qualcomm.com/company/product-security/bulletins/july-2020-bulletin	H-QUA-MSM8-190820/1520

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables in APQ8009, APQ8017, APQ8053, APQ8096AU, APQ8098, Kamorta, MDM9206, MDM9207C, MDM9607, MSM8905, MSM8909W, MSM8917, MSM8920, MSM8937, MSM8940, MSM8953, MSM8996, MSM8996AU, MSM8998, Nicobar, QCA6574AU, QCM2150, QCS405, QCS605, QM215, Rennell, SA6155P, Saipan, SDA660, SDA845, SDM429, SDM429W, SDM439, SDM450, SDM630, SDM632, SDM636, SDM660, SDM670, SDM710, SDM845, SDX20, SM6150, SM7150, SM8150, SM8250, SXR1130, SXR2130 **CVE ID : CVE-2020-3688**		
Out-of-bounds Write	30-Jul-20	7.5	Out of bound write while QoS DSCP mapping due to improper input validation for data received from association response frame in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables in	https://www.qualcomm.com/company/product-security/bulletins/july-2020-bulletin	H-QUA-MSM8-190820/1521

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			APQ8009, APQ8017, APQ8053, APQ8096AU, APQ8098, MDM9150, MDM9206, MDM9207C, MDM9607, MDM9650, MSM8905, MSM8909W, MSM8917, MSM8920, MSM8937, MSM8940, MSM8953, MSM8996AU, Nicobar, QCA6174A, QCA6574AU, QCA9377, QCA9379, QCM2150, QCN7605, QCS405, QCS605, QM215, SA6155P, Saipan, SC8180X, SDA845, SDM429, SDM429W, SDM439, SDM450, SDM630, SDM632, SDM636, SDM660, SDM845, SDX20, SDX55, SM8150, SM8250, SXR2130 **CVE ID : CVE-2020-3698**		
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	30-Jul-20	7.5	Possible out of bound access while processing assoc response from host due to improper length check before copying into buffer 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,	https://www.qualcomm.com/company/product-security/bulletins/july-2020-bulletin	H-QUA-MSM8-190820/1522

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			MDM9650, MSM8905, MSM8909W, MSM8917, MSM8920, MSM8937, MSM8940, MSM8953, MSM8996AU, Nicobar, QCA6174A, QCA6574AU, QCA9377, QCA9379, QCM2150, QCN7605, QCS405, QCS605, QM215, SA6155P, Saipan, SC8180X, SDA845, SDM429, SDM429W, SDM439, SDM450, SDM630, SDM632, SDM636, SDM660, SDM845, SDX20, SDX55, SM6150, SM7150, SM8150, SM8250, SXR2130 **CVE ID : CVE-2020-3699**		
msm8998					
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	30-Jul-20	7.5	Possible buffer overflow while parsing mp4 clip with corrupted sample atoms due to improper validation of index in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables in APQ8009, APQ8017, APQ8053, APQ8096AU, APQ8098, Kamorta, MDM9206, MDM9207C, MDM9607, MSM8905, MSM8909W, MSM8917,	https://www.qualcomm.com/company/product-security/bulletins/july-2020-bulletin	H-QUA-MSM8-190820/1523

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			MSM8920, MSM8937, MSM8940, MSM8953, MSM8996, MSM8996AU, MSM8998, Nicobar, QCA6574AU, QCM2150, QCS405, QCS605, QM215, Rennell, SA6155P, Saipan, SDA660, SDA845, SDM429, SDM429W, SDM439, SDM450, SDM630, SDM632, SDM636, SDM660, SDM670, SDM710, SDM845, SDX20, SM6150, SM7150, SM8150, SM8250, SXR1130, SXR2130 **CVE ID : CVE-2020-3688**		
nicobar					
Use After Free	30-Jul-20	7.5	Use-after-free issue could occur due to dangling pointer when generating a frame buffer in OpenGL ES in Snapdragon Compute, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music in APQ8009, Nicobar, QCM2150, QCS405, Saipan, SDM845, SM8150, SM8250, SXR2130 **CVE ID : CVE-2020-3671**	https://www.qualcomm.com/company/product-security/bulletins/july-2020-bulletin	H-QUA-NICO-190820/1524
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	30-Jul-20	7.5	Possible buffer overflow while parsing mp4 clip with corrupted sample atoms due to improper validation of index in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity,	https://www.qualcomm.com/company/product-security/bulletins/july-2020-	H-QUA-NICO-190820/1525

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, APQ8098, Kamorta, MDM9206, MDM9207C, MDM9607, MSM8905, MSM8909W, MSM8917, MSM8920, MSM8937, MSM8940, MSM8953, MSM8996, MSM8996AU, MSM8998, Nicobar, QCA6574AU, QCM2150, QCS405, QCS605, QM215, Rennell, SA6155P, Saipan, SDA660, SDA845, SDM429, SDM429W, SDM439, SDM450, SDM630, SDM632, SDM636, SDM660, SDM670, SDM710, SDM845, SDX20, SM6150, SM7150, SM8150, SM8250, SXR1130, SXR2130 **CVE ID : CVE-2020-3688**	bulletin	
Out-of-bounds Write	30-Jul-20	7.5	Out of bound write while QoS DSCP mapping due to improper input validation for data received from association response frame in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music,	https://www.qualcomm.com/company/product-security/bulletins/july-2020-bulletin	H-QUA-NICO-190820/1526

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Snapdragon Wearables in APQ8009, APQ8017, APQ8053, APQ8096AU, APQ8098, MDM9150, MDM9206, MDM9207C, MDM9607, MDM9650, MSM8905, MSM8909W, MSM8917, MSM8920, MSM8937, MSM8940, MSM8953, MSM8996AU, Nicobar, QCA6174A, QCA6574AU, QCA9377, QCA9379, QCM2150, QCN7605, QCS405, QCS605, QM215, SA6155P, Saipan, SC8180X, SDA845, SDM429, SDM429W, SDM439, SDM450, SDM630, SDM632, SDM636, SDM660, SDM845, SDX20, SDX55, SM8150, SM8250, SXR2130 **CVE ID : CVE-2020-3698**		
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	30-Jul-20	7.5	Possible out of bound access while processing assoc response from host due to improper length check before copying into buffer 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,	https://www.qualcomm.com/company/product-security/bulletins/july-2020-bulletin	H-QUA-NICO-190820/1527

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			MDM9607, MDM9640, MDM9650, MSM8905, MSM8909W, MSM8917, MSM8920, MSM8937, MSM8940, MSM8953, MSM8996AU, Nicobar, QCA6174A, QCA6574AU, QCA9377, QCA9379, QCM2150, QCN7605, QCS405, QCS605, QM215, SA6155P, Saipan, SC8180X, SDA845, SDM429, SDM429W, SDM439, SDM450, SDM630, SDM632, SDM636, SDM660, SDM845, SDX20, SDX55, SM6150, SM7150, SM8150, SM8250, SXR2130 **CVE ID : CVE-2020-3699**		
apq8053					
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	30-Jul-20	7.5	Possible buffer overflow while parsing mp4 clip with corrupted sample atoms due to improper validation of index in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables in APQ8009, APQ8017, APQ8053, APQ8096AU, APQ8098, Kamorta, MDM9206, MDM9207C, MDM9607, MSM8905,	https://www.qualcomm.com/company/product-security/bulletins/july-2020-bulletin	H-QUA-APQ8-190820/1528

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			MSM8909W, MSM8917, MSM8920, MSM8937, MSM8940, MSM8953, MSM8996, MSM8996AU, MSM8998, Nicobar, QCA6574AU, QCM2150, QCS405, QCS605, QM215, Rennell, SA6155P, Saipan, SDA660, SDA845, SDM429, SDM429W, SDM439, SDM450, SDM630, SDM632, SDM636, SDM660, SDM670, SDM710, SDM845, SDX20, SM6150, SM7150, SM8150, SM8250, SXR1130, SXR2130 **CVE ID : CVE-2020-3688**		
Out-of-bounds Write	30-Jul-20	7.5	Out of bound write while QoS DSCP mapping due to improper input validation for data received from association response frame 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, APQ8098, MDM9150, MDM9206, MDM9207C, MDM9607, MDM9650, MSM8905, MSM8909W, MSM8917, MSM8920, MSM8937, MSM8940, MSM8953, MSM8996AU,	https://www.qualcomm.com/company/product-security/bulletins/july-2020-bulletin	H-QUA-APQ8-190820/1529

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Nicobar, QCA6174A, QCA6574AU, QCA9377, QCA9379, QCM2150, QCN7605, QCS405, QCS605, QM215, SA6155P, Saipan, SC8180X, SDA845, SDM429, SDM429W, SDM439, SDM450, SDM630, SDM632, SDM636, SDM660, SDM845, SDX20, SDX55, SM8150, SM8250, SXR2130 **CVE ID : CVE-2020-3698**		
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	30-Jul-20	7.5	Possible out of bound access while processing assoc response from host due to improper length check before copying into buffer 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, Nicobar, QCA6174A, QCA6574AU, QCA9377, QCA9379, QCM2150, QCN7605, QCS405, QCS605, QM215,	https://www.qualcomm.com/company/product-security/bulletins/july-2020-bulletin	H-QUA-APQ8-190820/1530

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			SA6155P, Saipan, SC8180X, SDA845, SDM429, SDM429W, SDM439, SDM450, SDM630, SDM632, SDM636, SDM660, SDM845, SDX20, SDX55, SM6150, SM7150, SM8150, SM8250, SXR2130 **CVE ID : CVE-2020-3699**		
Out-of-bounds Read	30-Jul-20	5	Possible out of bounds read due to a missing bounds check and could lead to local information disclosure in the wifi driver with no additional execution privileges needed in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking in APQ8053, APQ8096AU, IPQ4019, IPQ8064, IPQ8074, MDM9607, MSM8909W, MSM8996AU, QCA6574AU, QCA9531, QCA9558, QCA9980, SC8180X, SDM439, SDX55, SM8150, SM8250, SXR2130 **CVE ID : CVE-2020-3700**	https://www.qualcomm.com/company/product-security/bulletins/july-2020-bulletin	H-QUA-APQ8-190820/1531
mdm9207c					

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	30-Jul-20	7.5	Possible buffer overflow while parsing mp4 clip with corrupted sample atoms due to improper validation of index in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables in APQ8009, APQ8017, APQ8053, APQ8096AU, APQ8098, Kamorta, MDM9206, MDM9207C, MDM9607, MSM8905, MSM8909W, MSM8917, MSM8920, MSM8937, MSM8940, MSM8953, MSM8996, MSM8996AU, MSM8998, Nicobar, QCA6574AU, QCM2150, QCS405, QCS605, QM215, Rennell, SA6155P, Saipan, SDA660, SDA845, SDM429, SDM429W, SDM439, SDM450, SDM630, SDM632, SDM636, SDM660, SDM670, SDM710, SDM845, SDX20, SM6150, SM7150, SM8150, SM8250, SXR1130, SXR2130 **CVE ID : CVE-2020-3688**	https://www.qualcomm.com/company/product-security/bulletins/july-2020-bulletin	H-QUA-MDM9-190820/1532
Out-of-bounds Write	30-Jul-20	7.5	Out of bound write while QoS DSCP mapping due to improper input validation for data received from association response	https://www.qualcomm.com/company/product-security/bull	H-QUA-MDM9-190820/1533

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			frame 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, APQ8098, MDM9150, MDM9206, MDM9207C, MDM9607, MDM9650, MSM8905, MSM8909W, MSM8917, MSM8920, MSM8937, MSM8940, MSM8953, MSM8996AU, Nicobar, QCA6174A, QCA6574AU, QCA9377, QCA9379, QCM2150, QCN7605, QCS405, QCS605, QM215, SA6155P, Saipan, SC8180X, SDA845, SDM429, SDM429W, SDM439, SDM450, SDM630, SDM632, SDM636, SDM660, SDM845, SDX20, SDX55, SM8150, SM8250, SXR2130 **CVE ID : CVE-2020-3698**	etins/july-2020-bulletin	
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	30-Jul-20	7.5	Possible out of bound access while processing assoc response from host due to improper length check before copying into buffer in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer Electronics Connectivity,	https://www.qualcomm.com/company/product-security/bulletins/july-2020-bulletin	H-QUA-MDM9-190820/1534

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, Nicobar, QCA6174A, QCA6574AU, QCA9377, QCA9379, QCM2150, QCN7605, QCS405, QCS605, QM215, SA6155P, Saipan, SC8180X, SDA845, SDM429, SDM429W, SDM439, SDM450, SDM630, SDM632, SDM636, SDM660, SDM845, SDX20, SDX55, SM6150, SM7150, SM8150, SM8250, SXR2130 **CVE ID : CVE-2020-3699**		
msm8905					
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	30-Jul-20	7.5	Possible buffer overflow while parsing mp4 clip with corrupted sample atoms due to improper validation of index in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial	https://www.qualcomm.com/company/product-security/bulletins/july-2020-bulletin	H-QUA-MSM8-190820/1535

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables in APQ8009, APQ8017, APQ8053, APQ8096AU, APQ8098, Kamorta, MDM9206, MDM9207C, MDM9607, MSM8905, MSM8909W, MSM8917, MSM8920, MSM8937, MSM8940, MSM8953, MSM8996, MSM8996AU, MSM8998, Nicobar, QCA6574AU, QCM2150, QCS405, QCS605, QM215, Rennell, SA6155P, Saipan, SDA660, SDA845, SDM429, SDM429W, SDM439, SDM450, SDM630, SDM632, SDM636, SDM660, SDM670, SDM710, SDM845, SDX20, SM6150, SM7150, SM8150, SM8250, SXR1130, SXR2130 **CVE ID : CVE-2020-3688**		
Out-of-bounds Write	30-Jul-20	7.5	Out of bound write while QoS DSCP mapping due to improper input validation for data received from association response frame 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,	https://www.qualcomm.com/company/product-security/bulletins/july-2020-bulletin	H-QUA-MSM8-190820/1536

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			APQ8053, APQ8096AU, APQ8098, MDM9150, MDM9206, MDM9207C, MDM9607, MDM9650, MSM8905, MSM8909W, MSM8917, MSM8920, MSM8937, MSM8940, MSM8953, MSM8996AU, Nicobar, QCA6174A, QCA6574AU, QCA9377, QCA9379, QCM2150, QCN7605, QCS405, QCS605, QM215, SA6155P, Saipan, SC8180X, SDA845, SDM429, SDM429W, SDM439, SDM450, SDM630, SDM632, SDM636, SDM660, SDM845, SDX20, SDX55, SM8150, SM8250, SXR2130 **CVE ID : CVE-2020-3698**		
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	30-Jul-20	7.5	Possible out of bound access while processing assoc response from host due to improper length check before copying into buffer 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,	https://www.qualcomm.com/company/product-security/bulletins/july-2020-bulletin	H-QUA-MSM8-190820/1537

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			MSM8909W, MSM8917, MSM8920, MSM8937, MSM8940, MSM8953, MSM8996AU, Nicobar, QCA6174A, QCA6574AU, QCA9377, QCA9379, QCM2150, QCN7605, QCS405, QCS605, QM215, SA6155P, Saipan, SC8180X, SDA845, SDM429, SDM429W, SDM439, SDM450, SDM630, SDM632, SDM636, SDM660, SDM845, SDX20, SDX55, SM6150, SM7150, SM8150, SM8250, SXR2130 **CVE ID : CVE-2020-3699**		
qcn7605					
Out-of-bounds Write	30-Jul-20	7.5	Out of bound write while QoS DSCP mapping due to improper input validation for data received from association response frame 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, APQ8098, MDM9150, MDM9206, MDM9207C, MDM9607, MDM9650, MSM8905, MSM8909W,	https://www.qualcomm.com/company/product-security/bulletins/july-2020-bulletin	H-QUA-QCN7-190820/1538

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			MSM8917, MSM8920, MSM8937, MSM8940, MSM8953, MSM8996AU, Nicobar, QCA6174A, QCA6574AU, QCA9377, QCA9379, QCM2150, QCN7605, QCS405, QCS605, QM215, SA6155P, Saipan, SC8180X, SDA845, SDM429, SDM429W, SDM439, SDM450, SDM630, SDM632, SDM636, SDM660, SDM845, SDX20, SDX55, SM8150, SM8250, SXR2130 **CVE ID : CVE-2020-3698**		
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	30-Jul-20	7.5	Possible out of bound access while processing assoc response from host due to improper length check before copying into buffer 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, Nicobar, QCA6174A, QCA6574AU,	https://www.qualcomm.com/company/product-security/bulletins/july-2020-bulletin	H-QUA-QCN7-190820/1539

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			QCA9377, QCA9379, QCM2150, QCN7605, QCS405, QCS605, QM215, SA6155P, Saipan, SC8180X, SDA845, SDM429, SDM429W, SDM439, SDM450, SDM630, SDM632, SDM636, SDM660, SDM845, SDX20, SDX55, SM6150, SM7150, SM8150, SM8250, SXR2130 **CVE ID : CVE-2020-3699**		
sdm845					
Use After Free	30-Jul-20	7.5	Use-after-free issue could occur due to dangling pointer when generating a frame buffer in OpenGL ES in Snapdragon Compute, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music in APQ8009, Nicobar, QCM2150, QCS405, Saipan, SDM845, SM8150, SM8250, SXR2130 **CVE ID : CVE-2020-3671**	https://www.qualcomm.com/company/product-security/bulletins/july-2020-bulletin	H-QUA-SDM8-190820/1540
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	30-Jul-20	7.5	Possible buffer overflow while parsing mp4 clip with corrupted sample atoms due to improper validation of index in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile,	https://www.qualcomm.com/company/product-security/bulletins/july-2020-bulletin	H-QUA-SDM8-190820/1541

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Snapdragon Voice & Music, Snapdragon Wearables in APQ8009, APQ8017, APQ8053, APQ8096AU, APQ8098, Kamorta, MDM9206, MDM9207C, MDM9607, MSM8905, MSM8909W, MSM8917, MSM8920, MSM8937, MSM8940, MSM8953, MSM8996, MSM8996AU, MSM8998, Nicobar, QCA6574AU, QCM2150, QCS405, QCS605, QM215, Rennell, SA6155P, Saipan, SDA660, SDA845, SDM429, SDM429W, SDM439, SDM450, SDM630, SDM632, SDM636, SDM660, SDM670, SDM710, SDM845, SDX20, SM6150, SM7150, SM8150, SM8250, SXR1130, SXR2130 **CVE ID : CVE-2020-3688**		
Out-of-bounds Write	30-Jul-20	7.5	Out of bound write while QoS DSCP mapping due to improper input validation for data received from association response frame 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,	https://www.qualcomm.com/company/product-security/bulletins/july-2020-bulletin	H-QUA-SDM8-190820/1542

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			APQ8098, MDM9150, MDM9206, MDM9207C, MDM9607, MDM9650, MSM8905, MSM8909W, MSM8917, MSM8920, MSM8937, MSM8940, MSM8953, MSM8996AU, Nicobar, QCA6174A, QCA6574AU, QCA9377, QCA9379, QCM2150, QCN7605, QCS405, QCS605, QM215, SA6155P, Saipan, SC8180X, SDA845, SDM429, SDM429W, SDM439, SDM450, SDM630, SDM632, SDM636, SDM660, SDM845, SDX20, SDX55, SM8150, SM8250, SXR2130 **CVE ID : CVE-2020-3698**		
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	30-Jul-20	7.5	Possible out of bound access while processing assoc response from host due to improper length check before copying into buffer 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,	https://www.qualcomm.com/company/product-security/bulletins/july-2020-bulletin	H-QUA-SDM8-190820/1543

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			MSM8920, MSM8937, MSM8940, MSM8953, MSM8996AU, Nicobar, QCA6174A, QCA6574AU, QCA9377, QCA9379, QCM2150, QCN7605, QCS405, QCS605, QM215, SA6155P, Saipan, SC8180X, SDA845, SDM429, SDM429W, SDM439, SDM450, SDM630, SDM632, SDM636, SDM660, SDM845, SDX20, SDX55, SM6150, SM7150, SM8150, SM8250, SXR2130 **CVE ID : CVE-2020-3699**		
apq8017					
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	30-Jul-20	7.5	Possible buffer overflow while parsing mp4 clip with corrupted sample atoms due to improper validation of index in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables in APQ8009, APQ8017, APQ8053, APQ8096AU, APQ8098, Kamorta, MDM9206, MDM9207C, MDM9607, MSM8905, MSM8909W, MSM8917, MSM8920, MSM8937, MSM8940, MSM8953,	https://www.qualcomm.com/company/product-security/bulletins/july-2020-bulletin	H-QUA-APQ8-190820/1544

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			MSM8996, MSM8996AU, MSM8998, Nicobar, QCA6574AU, QCM2150, QCS405, QCS605, QM215, Rennell, SA6155P, Saipan, SDA660, SDA845, SDM429, SDM429W, SDM439, SDM450, SDM630, SDM632, SDM636, SDM660, SDM670, SDM710, SDM845, SDX20, SM6150, SM7150, SM8150, SM8250, SXR1130, SXR2130 **CVE ID : CVE-2020-3688**		
Out-of-bounds Write	30-Jul-20	7.5	Out of bound write while QoS DSCP mapping due to improper input validation for data received from association response frame 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, APQ8098, MDM9150, MDM9206, MDM9207C, MDM9607, MDM9650, MSM8905, MSM8909W, MSM8917, MSM8920, MSM8937, MSM8940, MSM8953, MSM8996AU, Nicobar, QCA6174A, QCA6574AU, QCA9377, QCA9379, QCM2150,	https://www.qualcomm.com/company/product-security/bulletins/july-2020-bulletin	H-QUA-APQ8-190820/1545

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			QCN7605, QCS405, QCS605, QM215, SA6155P, Saipan, SC8180X, SDA845, SDM429, SDM429W, SDM439, SDM450, SDM630, SDM632, SDM636, SDM660, SDM845, SDX20, SDX55, SM8150, SM8250, SXR2130 **CVE ID : CVE-2020-3698**		
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	30-Jul-20	7.5	Possible out of bound access while processing assoc response from host due to improper length check before copying into buffer 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, Nicobar, QCA6174A, QCA6574AU, QCA9377, QCA9379, QCM2150, QCN7605, QCS405, QCS605, QM215, SA6155P, Saipan, SC8180X, SDA845, SDM429, SDM429W,	https://www.qualcomm.com/company/product-security/bulletins/july-2020-bulletin	H-QUA-APQ8-190820/1546

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			SDM439, SDM450, SDM630, SDM632, SDM636, SDM660, SDM845, SDX20, SDX55, SM6150, SM7150, SM8150, SM8250, SXR2130 **CVE ID : CVE-2020-3699**		
apq8096au					
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	30-Jul-20	7.5	Possible buffer overflow while parsing mp4 clip with corrupted sample atoms due to improper validation of index in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables in APQ8009, APQ8017, APQ8053, APQ8096AU, APQ8098, Kamorta, MDM9206, MDM9207C, MDM9607, MSM8905, MSM8909W, MSM8917, MSM8920, MSM8937, MSM8940, MSM8953, MSM8996, MSM8996AU, MSM8998, Nicobar, QCA6574AU, QCM2150, QCS405, QCS605, QM215, Rennell, SA6155P, Saipan, SDA660, SDA845, SDM429, SDM429W, SDM439, SDM450, SDM630, SDM632, SDM636, SDM660, SDM670,	https://www.qualcomm.com/company/product-security/bulletins/july-2020-bulletin	H-QUA-APQ8-190820/1547

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			SDM710, SDM845, SDX20, SM6150, SM7150, SM8150, SM8250, SXR1130, SXR2130 **CVE ID : CVE-2020-3688**		
Out-of-bounds Write	30-Jul-20	7.5	Out of bound write while QoS DSCP mapping due to improper input validation for data received from association response frame 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, APQ8098, MDM9150, MDM9206, MDM9207C, MDM9607, MDM9650, MSM8905, MSM8909W, MSM8917, MSM8920, MSM8937, MSM8940, MSM8953, MSM8996AU, Nicobar, QCA6174A, QCA6574AU, QCA9377, QCA9379, QCM2150, QCN7605, QCS405, QCS605, QM215, SA6155P, Saipan, SC8180X, SDA845, SDM429, SDM429W, SDM439, SDM450, SDM630, SDM632, SDM636, SDM660, SDM845, SDX20, SDX55, SM8150, SM8250,	https://www.qualcomm.com/company/product-security/bulletins/july-2020-bulletin	H-QUA-APQ8-190820/1548

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			SXR2130 **CVE ID : CVE-2020-3698**		
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	30-Jul-20	7.5	Possible out of bound access while processing assoc response from host due to improper length check before copying into buffer 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, Nicobar, QCA6174A, QCA6574AU, QCA9377, QCA9379, QCM2150, QCN7605, QCS405, QCS605, QM215, SA6155P, Saipan, SC8180X, SDA845, SDM429, SDM429W, SDM439, SDM450, SDM630, SDM632, SDM636, SDM660, SDM845, SDX20, SDX55, SM6150, SM7150, SM8150, SM8250, SXR2130 **CVE ID : CVE-2020-3699**	https://www.qualcomm.com/company/product-security/bulletins/july-2020-bulletin	H-QUA-APQ8-190820/1549

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Out-of-bounds Read	30-Jul-20	5	Possible out of bounds read due to a missing bounds check and could lead to local information disclosure in the wifi driver with no additional execution privileges needed in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking in APQ8053, APQ8096AU, IPQ4019, IPQ8064, IPQ8074, MDM9607, MSM8909W, MSM8996AU, QCA6574AU, QCA9531, QCA9558, QCA9980, SC8180X, SDM439, SDX55, SM8150, SM8250, SXR2130 **CVE ID : CVE-2020-3700**	https://www.qualcomm.com/company/product-security/bulletins/july-2020-bulletin	H-QUA-APQ8-190820/1550
sda845					
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	30-Jul-20	7.5	Possible buffer overflow while parsing mp4 clip with corrupted sample atoms due to improper validation of index in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music,	https://www.qualcomm.com/company/product-security/bulletins/july-2020-bulletin	H-QUA-SDA8-190820/1551

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Snapdragon Wearables in APQ8009, APQ8017, APQ8053, APQ8096AU, APQ8098, Kamorta, MDM9206, MDM9207C, MDM9607, MSM8905, MSM8909W, MSM8917, MSM8920, MSM8937, MSM8940, MSM8953, MSM8996, MSM8996AU, MSM8998, Nicobar, QCA6574AU, QCM2150, QCS405, QCS605, QM215, Rennell, SA6155P, Saipan, SDA660, SDA845, SDM429, SDM429W, SDM439, SDM450, SDM630, SDM632, SDM636, SDM660, SDM670, SDM710, SDM845, SDX20, SM6150, SM7150, SM8150, SM8250, SXR1130, SXR2130 **CVE ID : CVE-2020-3688**		
Out-of-bounds Write	30-Jul-20	7.5	Out of bound write while QoS DSCP mapping due to improper input validation for data received from association response frame 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, APQ8098, MDM9150,	https://www.qualcomm.com/company/product-security/bulletins/july-2020-bulletin	H-QUA-SDA8-190820/1552

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			MDM9206, MDM9207C, MDM9607, MDM9650, MSM8905, MSM8909W, MSM8917, MSM8920, MSM8937, MSM8940, MSM8953, MSM8996AU, Nicobar, QCA6174A, QCA6574AU, QCA9377, QCA9379, QCM2150, QCN7605, QCS405, QCS605, QM215, SA6155P, Saipan, SC8180X, SDA845, SDM429, SDM429W, SDM439, SDM450, SDM630, SDM632, SDM636, SDM660, SDM845, SDX20, SDX55, SM8150, SM8250, SXR2130 **CVE ID : CVE-2020-3698**		
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	30-Jul-20	7.5	Possible out of bound access while processing assoc response from host due to improper length check before copying into buffer 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,	https://www.qualcomm.com/company/product-security/bulletins/july-2020-bulletin	H-QUA-SDA8-190820/1553

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			MSM8940, MSM8953, MSM8996AU, Nicobar, QCA6174A, QCA6574AU, QCA9377, QCA9379, QCM2150, QCN7605, QCS405, QCS605, QM215, SA6155P, Saipan, SC8180X, SDA845, SDM429, SDM429W, SDM439, SDM450, SDM630, SDM632, SDM636, SDM660, SDM845, SDX20, SDX55, SM6150, SM7150, SM8150, SM8250, SXR2130 **CVE ID : CVE-2020-3699**		
sdm636					
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	30-Jul-20	7.5	Possible buffer overflow while parsing mp4 clip with corrupted sample atoms due to improper validation of index in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables in APQ8009, APQ8017, APQ8053, APQ8096AU, APQ8098, Kamorta, MDM9206, MDM9207C, MDM9607, MSM8905, MSM8909W, MSM8917, MSM8920, MSM8937, MSM8940, MSM8953, MSM8996, MSM8996AU,	https://www.qualcomm.com/company/product-security/bulletins/july-2020-bulletin	H-QUA-SDM6-190820/1554

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			MSM8998, Nicobar, QCA6574AU, QCM2150, QCS405, QCS605, QM215, Rennell, SA6155P, Saipan, SDA660, SDA845, SDM429, SDM429W, SDM439, SDM450, SDM630, SDM632, SDM636, SDM660, SDM670, SDM710, SDM845, SDX20, SM6150, SM7150, SM8150, SM8250, SXR1130, SXR2130 **CVE ID : CVE-2020-3688**		
Out-of-bounds Write	30-Jul-20	7.5	Out of bound write while QoS DSCP mapping due to improper input validation for data received from association response frame 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, APQ8098, MDM9150, MDM9206, MDM9207C, MDM9607, MDM9650, MSM8905, MSM8909W, MSM8917, MSM8920, MSM8937, MSM8940, MSM8953, MSM8996AU, Nicobar, QCA6174A, QCA6574AU, QCA9377, QCA9379, QCM2150, QCN7605, QCS405,	https://www.qualcomm.com/company/product-security/bulletins/july-2020-bulletin	H-QUA-SDM6-190820/1555

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			QCS605, QM215, SA6155P, Saipan, SC8180X, SDA845, SDM429, SDM429W, SDM439, SDM450, SDM630, SDM632, SDM636, SDM660, SDM845, SDX20, SDX55, SM8150, SM8250, SXR2130 **CVE ID : CVE-2020-3698**		
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	30-Jul-20	7.5	Possible out of bound access while processing assoc response from host due to improper length check before copying into buffer 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, Nicobar, QCA6174A, QCA6574AU, QCA9377, QCA9379, QCM2150, QCN7605, QCS405, QCS605, QM215, SA6155P, Saipan, SC8180X, SDA845, SDM429, SDM429W, SDM439, SDM450,	https://www.qualcomm.com/company/product-security/bulletins/july-2020-bulletin	H-QUA-SDM6-190820/1556

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			SDM630, SDM632, SDM636, SDM660, SDM845, SDX20, SDX55, SM6150, SM7150, SM8150, SM8250, SXR2130 **CVE ID : CVE-2020-3699**		
sdm670					
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	30-Jul-20	7.5	Possible buffer overflow while parsing mp4 clip with corrupted sample atoms due to improper validation of index in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables in APQ8009, APQ8017, APQ8053, APQ8096AU, APQ8098, Kamorta, MDM9206, MDM9207C, MDM9607, MSM8905, MSM8909W, MSM8917, MSM8920, MSM8937, MSM8940, MSM8953, MSM8996, MSM8996AU, MSM8998, Nicobar, QCA6574AU, QCM2150, QCS405, QCS605, QM215, Rennell, SA6155P, Saipan, SDA660, SDA845, SDM429, SDM429W, SDM439, SDM450, SDM630, SDM632, SDM636, SDM660, SDM670, SDM710, SDM845, SDX20,	https://www.qualcomm.com/company/product-security/bulletins/july-2020-bulletin	H-QUA-SDM6-190820/1557

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			SM6150, SM7150, SM8150, SM8250, SXR1130, SXR2130 **CVE ID : CVE-2020-3688**		
sdm710					
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	30-Jul-20	7.5	Possible buffer overflow while parsing mp4 clip with corrupted sample atoms due to improper validation of index in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables in APQ8009, APQ8017, APQ8053, APQ8096AU, APQ8098, Kamorta, MDM9206, MDM9207C, MDM9607, MSM8905, MSM8909W, MSM8917, MSM8920, MSM8937, MSM8940, MSM8953, MSM8996, MSM8996AU, MSM8998, Nicobar, QCA6574AU, QCM2150, QCS405, QCS605, QM215, Rennell, SA6155P, Saipan, SDA660, SDA845, SDM429, SDM429W, SDM439, SDM450, SDM630, SDM632, SDM636, SDM660, SDM670, SDM710, SDM845, SDX20, SM6150, SM7150, SM8150, SM8250, SXR1130, SXR2130	https://www.qualcomm.com/company/product-security/bulletins/july-2020-bulletin	H-QUA-SDM7-190820/1558

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2020-3688		
sxr1130					
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	30-Jul-20	7.5	Possible buffer overflow while parsing mp4 clip with corrupted sample atoms due to improper validation of index in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables in APQ8009, APQ8017, APQ8053, APQ8096AU, APQ8098, Kamorta, MDM9206, MDM9207C, MDM9607, MSM8905, MSM8909W, MSM8917, MSM8920, MSM8937, MSM8940, MSM8953, MSM8996, MSM8996AU, MSM8998, Nicobar, QCA6574AU, QCM2150, QCS405, QCS605, QM215, Rennell, SA6155P, Saipan, SDA660, SDA845, SDM429, SDM429W, SDM439, SDM450, SDM630, SDM632, SDM636, SDM660, SDM670, SDM710, SDM845, SDX20, SM6150, SM7150, SM8150, SM8250, SXR1130, SXR2130 **CVE ID : CVE-2020-3688**	https://www.qualcomm.com/company/product-security/bulletins/july-2020-bulletin	H-QUA-SXR1-190820/1559
sm6150					

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	30-Jul-20	7.5	Possible buffer overflow while parsing mp4 clip with corrupted sample atoms due to improper validation of index in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables in APQ8009, APQ8017, APQ8053, APQ8096AU, APQ8098, Kamorta, MDM9206, MDM9207C, MDM9607, MSM8905, MSM8909W, MSM8917, MSM8920, MSM8937, MSM8940, MSM8953, MSM8996, MSM8996AU, MSM8998, Nicobar, QCA6574AU, QCM2150, QCS405, QCS605, QM215, Rennell, SA6155P, Saipan, SDA660, SDA845, SDM429, SDM429W, SDM439, SDM450, SDM630, SDM632, SDM636, SDM660, SDM670, SDM710, SDM845, SDX20, SM6150, SM7150, SM8150, SM8250, SXR1130, SXR2130 **CVE ID : CVE-2020-3688**	https://www.qualcomm.com/company/product-security/bulletins/july-2020-bulletin	H-QUA-SM61-190820/1560
Buffer Copy without Checking Size of Input ('Classic	30-Jul-20	7.5	Possible out of bound access while processing assoc response from host due to improper length check before copying into	https://www.qualcomm.com/company/product-security/bull	H-QUA-SM61-190820/1561

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Buffer Overflow')			buffer 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, Nicobar, QCA6174A, QCA6574AU, QCA9377, QCA9379, QCM2150, QCN7605, QCS405, QCS605, QM215, SA6155P, Saipan, SC8180X, SDA845, SDM429, SDM429W, SDM439, SDM450, SDM630, SDM632, SDM636, SDM660, SDM845, SDX20, SDX55, SM6150, SM7150, SM8150, SM8250, SXR2130 **CVE ID : CVE-2020-3699**	etins/july-2020-bulletin	
sm8150					
Use After Free	30-Jul-20	7.5	Use-after-free issue could occur due to dangling pointer when generating a frame buffer in OpenGL ES in Snapdragon Compute, Snapdragon Consumer	https://www.qualcomm.com/company/product-security/bulletins/july-	H-QUA-SM81-190820/1562

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music in APQ8009, Nicobar, QCM2150, QCS405, Saipan, SDM845, SM8150, SM8250, SXR2130 **CVE ID : CVE-2020-3671**	2020-bulletin	
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	30-Jul-20	7.5	Possible buffer overflow while parsing mp4 clip with corrupted sample atoms due to improper validation of index in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables in APQ8009, APQ8017, APQ8053, APQ8096AU, APQ8098, Kamorta, MDM9206, MDM9207C, MDM9607, MSM8905, MSM8909W, MSM8917, MSM8920, MSM8937, MSM8940, MSM8953, MSM8996, MSM8996AU, MSM8998, Nicobar, QCA6574AU, QCM2150, QCS405, QCS605, QM215, Rennell, SA6155P, Saipan, SDA660, SDA845, SDM429, SDM429W, SDM439, SDM450, SDM630, SDM632, SDM636, SDM660, SDM670, SDM710, SDM845, SDX20, SM6150, SM7150,	https://www.qualcomm.com/company/product-security/bulletins/july-2020-bulletin	H-QUA-SM81-190820/1563

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			SM8150, SM8250, SXR1130, SXR2130 **CVE ID : CVE-2020-3688**		
Out-of-bounds Write	30-Jul-20	7.5	Out of bound write while QoS DSCP mapping due to improper input validation for data received from association response frame 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, APQ8098, MDM9150, MDM9206, MDM9207C, MDM9607, MDM9650, MSM8905, MSM8909W, MSM8917, MSM8920, MSM8937, MSM8940, MSM8953, MSM8996AU, Nicobar, QCA6174A, QCA6574AU, QCA9377, QCA9379, QCM2150, QCN7605, QCS405, QCS605, QM215, SA6155P, Saipan, SC8180X, SDA845, SDM429, SDM429W, SDM439, SDM450, SDM630, SDM632, SDM636, SDM660, SDM845, SDX20, SDX55, SM8150, SM8250, SXR2130 **CVE ID : CVE-2020-3698**	https://www.qualcomm.com/company/product-security/bulletins/july-2020-bulletin	H-QUA-SM81-190820/1564

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

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	30-Jul-20	7.5	Possible out of bound access while processing assoc response from host due to improper length check before copying into buffer 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, Nicobar, QCA6174A, QCA6574AU, QCA9377, QCA9379, QCM2150, QCN7605, QCS405, QCS605, QM215, SA6155P, Saipan, SC8180X, SDA845, SDM429, SDM429W, SDM439, SDM450, SDM630, SDM632, SDM636, SDM660, SDM845, SDX20, SDX55, SM6150, SM7150, SM8150, SM8250, SXR2130 **CVE ID : CVE-2020-3699**	https://www.qualcomm.com/company/product-security/bulletins/july-2020-bulletin	H-QUA-SM81-190820/1565
Out-of-bounds Read	30-Jul-20	5	Possible out of bounds read due to a missing bounds check and could	https://www.qualcomm.com/compan	H-QUA-SM81-190820/1566

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			lead to local information disclosure in the wifi driver with no additional execution privileges needed in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking in APQ8053, APQ8096AU, IPQ4019, IPQ8064, IPQ8074, MDM9607, MSM8909W, MSM8996AU, QCA6574AU, QCA9531, QCA9558, QCA9980, SC8180X, SDM439, SDX55, SM8150, SM8250, SXR2130 **CVE ID : CVE-2020-3700**	y/product-security/bulletins/july-2020-bulletin	
qca9531					
Out-of-bounds Read	30-Jul-20	5	Possible out of bounds read due to a missing bounds check and could lead to local information disclosure in the wifi driver with no additional execution privileges needed in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables,	https://www.qualcomm.com/company/product-security/bulletins/july-2020-bulletin	H-QUA-QCA9-190820/1567

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Snapdragon Wired Infrastructure and Networking in APQ8053, APQ8096AU, IPQ4019, IPQ8064, IPQ8074, MDM9607, MSM8909W, MSM8996AU, QCA6574AU, QCA9531, QCA9558, QCA9980, SC8180X, SDM439, SDX55, SM8150, SM8250, SXR2130 **CVE ID : CVE-2020-3700**		
qca9980					
Out-of-bounds Read	30-Jul-20	5	Possible out of bounds read due to a missing bounds check and could lead to local information disclosure in the wifi driver with no additional execution privileges needed in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking in APQ8053, APQ8096AU, IPQ4019, IPQ8064, IPQ8074, MDM9607, MSM8909W, MSM8996AU, QCA6574AU, QCA9531, QCA9558, QCA9980, SC8180X, SDM439, SDX55, SM8150, SM8250, SXR2130 **CVE ID : CVE-2020-3700**	https://www.qualcomm.com/company/product-security/bulletins/july-2020-bulletin	H-QUA-QCA9-190820/1568

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
qm215					
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	30-Jul-20	7.5	Possible buffer overflow while parsing mp4 clip with corrupted sample atoms due to improper validation of index in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables in APQ8009, APQ8017, APQ8053, APQ8096AU, APQ8098, Kamorta, MDM9206, MDM9207C, MDM9607, MSM8905, MSM8909W, MSM8917, MSM8920, MSM8937, MSM8940, MSM8953, MSM8996, MSM8996AU, MSM8998, Nicobar, QCA6574AU, QCM2150, QCS405, QCS605, QM215, Rennell, SA6155P, Saipan, SDA660, SDA845, SDM429, SDM429W, SDM439, SDM450, SDM630, SDM632, SDM636, SDM660, SDM670, SDM710, SDM845, SDX20, SM6150, SM7150, SM8150, SM8250, SXR1130, SXR2130 **CVE ID : CVE-2020-3688**	https://www.qualcomm.com/company/product-security/bulletins/july-2020-bulletin	H-QUA-QM21-190820/1569
Out-of-bounds Write	30-Jul-20	7.5	Out of bound write while QoS DSCP mapping due to improper input validation	https://www.qualcomm.com/compan	H-QUA-QM21-190820/1570

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			for data received from association response frame 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, APQ8098, MDM9150, MDM9206, MDM9207C, MDM9607, MDM9650, MSM8905, MSM8909W, MSM8917, MSM8920, MSM8937, MSM8940, MSM8953, MSM8996AU, Nicobar, QCA6174A, QCA6574AU, QCA9377, QCA9379, QCM2150, QCN7605, QCS405, QCS605, QM215, SA6155P, Saipan, SC8180X, SDA845, SDM429, SDM429W, SDM439, SDM450, SDM630, SDM632, SDM636, SDM660, SDM845, SDX20, SDX55, SM8150, SM8250, SXR2130 **CVE ID : CVE-2020-3698**	y/product-security/bulletins/july-2020-bulletin	
Buffer Copy without Checking Size of Input ('Classic Buffer	30-Jul-20	7.5	Possible out of bound access while processing assoc response from host due to improper length check before copying into buffer in Snapdragon Auto, Snapdragon Compute,	https://www.qualcomm.com/company/product-security/bulletins/july-2020-	H-QUA-QM21-190820/1571

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Overflow')			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, Nicobar, QCA6174A, QCA6574AU, QCA9377, QCA9379, QCM2150, QCN7605, QCS405, QCS605, QM215, SA6155P, Saipan, SC8180X, SDA845, SDM429, SDM429W, SDM439, SDM450, SDM630, SDM632, SDM636, SDM660, SDM845, SDX20, SDX55, SM6150, SM7150, SM8150, SM8250, SXR2130 **CVE ID : CVE-2020-3699**	bulletin	
sm7150					
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	30-Jul-20	7.5	Possible buffer overflow while parsing mp4 clip with corrupted sample atoms due to improper validation of index in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity,	https://www.qualcomm.com/company/product-security/bulletins/july-2020-bulletin	H-QUA-SM71-190820/1572

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, APQ8098, Kamorta, MDM9206, MDM9207C, MDM9607, MSM8905, MSM8909W, MSM8917, MSM8920, MSM8937, MSM8940, MSM8953, MSM8996, MSM8996AU, MSM8998, Nicobar, QCA6574AU, QCM2150, QCS405, QCS605, QM215, Rennell, SA6155P, Saipan, SDA660, SDA845, SDM429, SDM429W, SDM439, SDM450, SDM630, SDM632, SDM636, SDM660, SDM670, SDM710, SDM845, SDX20, SM6150, SM7150, SM8150, SM8250, SXR1130, SXR2130 **CVE ID : CVE-2020-3688**		
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	30-Jul-20	7.5	Possible out of bound access while processing assoc response from host due to improper length check before copying into buffer in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music,	https://www.qualcomm.com/company/product-security/bulletins/july-2020-bulletin	H-QUA-SM71-190820/1573

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Snapdragon Wearables in APQ8009, APQ8017, APQ8053, APQ8096AU, MDM9206, MDM9207C, MDM9607, MDM9640, MDM9650, MSM8905, MSM8909W, MSM8917, MSM8920, MSM8937, MSM8940, MSM8953, MSM8996AU, Nicobar, QCA6174A, QCA6574AU, QCA9377, QCA9379, QCM2150, QCN7605, QCS405, QCS605, QM215, SA6155P, Saipan, SC8180X, SDA845, SDM429, SDM429W, SDM439, SDM450, SDM630, SDM632, SDM636, SDM660, SDM845, SDX20, SDX55, SM6150, SM7150, SM8150, SM8250, SXR2130 **CVE ID : CVE-2020-3699**		
sdm429					
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	30-Jul-20	7.5	Possible buffer overflow while parsing mp4 clip with corrupted sample atoms due to improper validation of index in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables in APQ8009, APQ8017,	https://www.qualcomm.com/company/product-security/bulletins/july-2020-bulletin	H-QUA-SDM4-190820/1574

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			APQ8053, APQ8096AU, APQ8098, Kamorta, MDM9206, MDM9207C, MDM9607, MSM8905, MSM8909W, MSM8917, MSM8920, MSM8937, MSM8940, MSM8953, MSM8996, MSM8996AU, MSM8998, Nicobar, QCA6574AU, QCM2150, QCS405, QCS605, QM215, Rennell, SA6155P, Saipan, SDA660, SDA845, SDM429, SDM429W, SDM439, SDM450, SDM630, SDM632, SDM636, SDM660, SDM670, SDM710, SDM845, SDX20, SM6150, SM7150, SM8150, SM8250, SXR1130, SXR2130 **CVE ID : CVE-2020-3688**		
Out-of-bounds Write	30-Jul-20	7.5	Out of bound write while QoS DSCP mapping due to improper input validation for data received from association response frame 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, APQ8098, MDM9150, MDM9206, MDM9207C, MDM9607, MDM9650,	https://www.qualcomm.com/company/product-security/bulletins/july-2020-bulletin	H-QUA-SDM4-190820/1575

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			MSM8905, MSM8909W, MSM8917, MSM8920, MSM8937, MSM8940, MSM8953, MSM8996AU, Nicobar, QCA6174A, QCA6574AU, QCA9377, QCA9379, QCM2150, QCN7605, QCS405, QCS605, QM215, SA6155P, Saipan, SC8180X, SDA845, SDM429, SDM429W, SDM439, SDM450, SDM630, SDM632, SDM636, SDM660, SDM845, SDX20, SDX55, SM8150, SM8250, SXR2130 **CVE ID : CVE-2020-3698**		
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	30-Jul-20	7.5	Possible out of bound access while processing assoc response from host due to improper length check before copying into buffer 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, Nicobar,	https://www.qualcomm.com/company/product-security/bulletins/july-2020-bulletin	H-QUA-SDM4-190820/1576

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			QCA6174A, QCA6574AU, QCA9377, QCA9379, QCM2150, QCN7605, QCS405, QCS605, QM215, SA6155P, Saipan, SC8180X, SDA845, SDM429, SDM429W, SDM439, SDM450, SDM630, SDM632, SDM636, SDM660, SDM845, SDX20, SDX55, SM6150, SM7150, SM8150, SM8250, SXR2130 **CVE ID : CVE-2020-3699**		
sdm632					
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	30-Jul-20	7.5	Possible buffer overflow while parsing mp4 clip with corrupted sample atoms due to improper validation of index in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables in APQ8009, APQ8017, APQ8053, APQ8096AU, APQ8098, Kamorta, MDM9206, MDM9207C, MDM9607, MSM8905, MSM8909W, MSM8917, MSM8920, MSM8937, MSM8940, MSM8953, MSM8996, MSM8996AU, MSM8998, Nicobar, QCA6574AU, QCM2150,	https://www.qualcomm.com/company/product-security/bulletins/july-2020-bulletin	H-QUA-SDM6-190820/1577

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			QCS405, QCS605, QM215, Rennell, SA6155P, Saipan, SDA660, SDA845, SDM429, SDM429W, SDM439, SDM450, SDM630, SDM632, SDM636, SDM660, SDM670, SDM710, SDM845, SDX20, SM6150, SM7150, SM8150, SM8250, SXR1130, SXR2130 **CVE ID : CVE-2020-3688**		
Out-of-bounds Write	30-Jul-20	7.5	Out of bound write while QoS DSCP mapping due to improper input validation for data received from association response frame 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, APQ8098, MDM9150, MDM9206, MDM9207C, MDM9607, MDM9650, MSM8905, MSM8909W, MSM8917, MSM8920, MSM8937, MSM8940, MSM8953, MSM8996AU, Nicobar, QCA6174A, QCA6574AU, QCA9377, QCA9379, QCM2150, QCN7605, QCS405, QCS605, QM215, SA6155P, Saipan, SC8180X, SDA845,	https://www.qualcomm.com/company/product-security/bulletins/july-2020-bulletin	H-QUA-SDM6-190820/1578

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			SDM429, SDM429W, SDM439, SDM450, SDM630, SDM632, SDM636, SDM660, SDM845, SDX20, SDX55, SM8150, SM8250, SXR2130 **CVE ID : CVE-2020-3698**		
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	30-Jul-20	7.5	Possible out of bound access while processing assoc response from host due to improper length check before copying into buffer 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, Nicobar, QCA6174A, QCA6574AU, QCA9377, QCA9379, QCM2150, QCN7605, QCS405, QCS605, QM215, SA6155P, Saipan, SC8180X, SDA845, SDM429, SDM429W, SDM439, SDM450, SDM630, SDM632, SDM636, SDM660,	https://www.qualcomm.com/company/product-security/bulletins/july-2020-bulletin	H-QUA-SDM6-190820/1579

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			SDM845, SDX20, SDX55, SM6150, SM7150, SM8150, SM8250, SXR2130 **CVE ID : CVE-2020-3699**		
msm8917					
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	30-Jul-20	7.5	Possible buffer overflow while parsing mp4 clip with corrupted sample atoms due to improper validation of index in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables in APQ8009, APQ8017, APQ8053, APQ8096AU, APQ8098, Kamorta, MDM9206, MDM9207C, MDM9607, MSM8905, MSM8909W, MSM8917, MSM8920, MSM8937, MSM8940, MSM8953, MSM8996, MSM8996AU, MSM8998, Nicobar, QCA6574AU, QCM2150, QCS405, QCS605, QM215, Rennell, SA6155P, Saipan, SDA660, SDA845, SDM429, SDM429W, SDM439, SDM450, SDM630, SDM632, SDM636, SDM660, SDM670, SDM710, SDM845, SDX20, SM6150, SM7150, SM8150, SM8250,	https://www.qualcomm.com/company/product-security/bulletins/july-2020-bulletin	H-QUA-MSM8-190820/1580

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			SXR1130, SXR2130 **CVE ID : CVE-2020-3688**		
Out-of-bounds Write	30-Jul-20	7.5	Out of bound write while QoS DSCP mapping due to improper input validation for data received from association response frame 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, APQ8098, MDM9150, MDM9206, MDM9207C, MDM9607, MDM9650, MSM8905, MSM8909W, MSM8917, MSM8920, MSM8937, MSM8940, MSM8953, MSM8996AU, Nicobar, QCA6174A, QCA6574AU, QCA9377, QCA9379, QCM2150, QCN7605, QCS405, QCS605, QM215, SA6155P, Saipan, SC8180X, SDA845, SDM429, SDM429W, SDM439, SDM450, SDM630, SDM632, SDM636, SDM660, SDM845, SDX20, SDX55, SM8150, SM8250, SXR2130 **CVE ID : CVE-2020-3698**	https://www.qualcomm.com/company/product-security/bulletins/july-2020-bulletin	H-QUA-MSM8-190820/1581
Buffer Copy	30-Jul-20	7.5	Possible out of bound	https://ww	H-QUA-

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
without Checking Size of Input ('Classic Buffer Overflow')			access while processing assoc response from host due to improper length check before copying into buffer 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, Nicobar, QCA6174A, QCA6574AU, QCA9377, QCA9379, QCM2150, QCN7605, QCS405, QCS605, QM215, SA6155P, Saipan, SC8180X, SDA845, SDM429, SDM429W, SDM439, SDM450, SDM630, SDM632, SDM636, SDM660, SDM845, SDX20, SDX55, SM6150, SM7150, SM8150, SM8250, SXR2130 **CVE ID : CVE-2020-3699**	w.qualcomm.com/company/product-security/bulletins/july-2020-bulletin	MSM8-190820/1582
msm8920					
Buffer Copy without	30-Jul-20	7.5	Possible buffer overflow while parsing mp4 clip	https://www.qualcomm.	H-QUA-MSM8-

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Checking Size of Input ('Classic Buffer Overflow')			with corrupted sample atoms due to improper validation of index in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables in APQ8009, APQ8017, APQ8053, APQ8096AU, APQ8098, Kamorta, MDM9206, MDM9207C, MDM9607, MSM8905, MSM8909W, MSM8917, MSM8920, MSM8937, MSM8940, MSM8953, MSM8996, MSM8996AU, MSM8998, Nicobar, QCA6574AU, QCM2150, QCS405, QCS605, QM215, Rennell, SA6155P, Saipan, SDA660, SDA845, SDM429, SDM429W, SDM439, SDM450, SDM630, SDM632, SDM636, SDM660, SDM670, SDM710, SDM845, SDX20, SM6150, SM7150, SM8150, SM8250, SXR1130, SXR2130 **CVE ID : CVE-2020-3688**	com/company/product-security/bulletins/july-2020-bulletin	190820/1583
Out-of-bounds Write	30-Jul-20	7.5	Out of bound write while QoS DSCP mapping due to improper input validation for data received from association response frame in Snapdragon Auto, Snapdragon Compute,	https://www.qualcomm.com/company/product-security/bulletins/july-2020-	H-QUA-MSM8-190820/1584

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables in APQ8009, APQ8017, APQ8053, APQ8096AU, APQ8098, MDM9150, MDM9206, MDM9207C, MDM9607, MDM9650, MSM8905, MSM8909W, MSM8917, MSM8920, MSM8937, MSM8940, MSM8953, MSM8996AU, Nicobar, QCA6174A, QCA6574AU, QCA9377, QCA9379, QCM2150, QCN7605, QCS405, QCS605, QM215, SA6155P, Saipan, SC8180X, SDA845, SDM429, SDM429W, SDM439, SDM450, SDM630, SDM632, SDM636, SDM660, SDM845, SDX20, SDX55, SM8150, SM8250, SXR2130 **CVE ID : CVE-2020-3698**	bulletin	
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	30-Jul-20	7.5	Possible out of bound access while processing assoc response from host due to improper length check before copying into buffer in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial	https://www.qualcomm.com/company/product-security/bulletins/july-2020-bulletin	H-QUA-MSM8-190820/1585

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			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, Nicobar, QCA6174A, QCA6574AU, QCA9377, QCA9379, QCM2150, QCN7605, QCS405, QCS605, QM215, SA6155P, Saipan, SC8180X, SDA845, SDM429, SDM429W, SDM439, SDM450, SDM630, SDM632, SDM636, SDM660, SDM845, SDX20, SDX55, SM6150, SM7150, SM8150, SM8250, SXR2130 **CVE ID : CVE-2020-3699**		
msm8937					
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	30-Jul-20	7.5	Possible buffer overflow while parsing mp4 clip with corrupted sample atoms due to improper validation of index in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music,	https://www.qualcomm.com/company/product-security/bulletins/july-2020-bulletin	H-QUA-MSM8-190820/1586

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Snapdragon Wearables in APQ8009, APQ8017, APQ8053, APQ8096AU, APQ8098, Kamorta, MDM9206, MDM9207C, MDM9607, MSM8905, MSM8909W, MSM8917, MSM8920, MSM8937, MSM8940, MSM8953, MSM8996, MSM8996AU, MSM8998, Nicobar, QCA6574AU, QCM2150, QCS405, QCS605, QM215, Rennell, SA6155P, Saipan, SDA660, SDA845, SDM429, SDM429W, SDM439, SDM450, SDM630, SDM632, SDM636, SDM660, SDM670, SDM710, SDM845, SDX20, SM6150, SM7150, SM8150, SM8250, SXR1130, SXR2130 **CVE ID : CVE-2020-3688**		
Out-of-bounds Write	30-Jul-20	7.5	Out of bound write while QoS DSCP mapping due to improper input validation for data received from association response frame 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, APQ8098, MDM9150,	https://www.qualcomm.com/company/product-security/bulletins/july-2020-bulletin	H-QUA-MSM8-190820/1587

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			MDM9206, MDM9207C, MDM9607, MDM9650, MSM8905, MSM8909W, MSM8917, MSM8920, MSM8937, MSM8940, MSM8953, MSM8996AU, Nicobar, QCA6174A, QCA6574AU, QCA9377, QCA9379, QCM2150, QCN7605, QCS405, QCS605, QM215, SA6155P, Saipan, SC8180X, SDA845, SDM429, SDM429W, SDM439, SDM450, SDM630, SDM632, SDM636, SDM660, SDM845, SDX20, SDX55, SM8150, SM8250, SXR2130 **CVE ID : CVE-2020-3698**		
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	30-Jul-20	7.5	Possible out of bound access while processing assoc response from host due to improper length check before copying into buffer 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,	https://www.qualcomm.com/company/product-security/bulletins/july-2020-bulletin	H-QUA-MSM8-190820/1588

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			MSM8940, MSM8953, MSM8996AU, Nicobar, QCA6174A, QCA6574AU, QCA9377, QCA9379, QCM2150, QCN7605, QCS405, QCS605, QM215, SA6155P, Saipan, SC8180X, SDA845, SDM429, SDM429W, SDM439, SDM450, SDM630, SDM632, SDM636, SDM660, SDM845, SDX20, SDX55, SM6150, SM7150, SM8150, SM8250, SXR2130 **CVE ID : CVE-2020-3699**		
msm8940					
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	30-Jul-20	7.5	Possible buffer overflow while parsing mp4 clip with corrupted sample atoms due to improper validation of index in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables in APQ8009, APQ8017, APQ8053, APQ8096AU, APQ8098, Kamorta, MDM9206, MDM9207C, MDM9607, MSM8905, MSM8909W, MSM8917, MSM8920, MSM8937, MSM8940, MSM8953, MSM8996, MSM8996AU,	https://www.qualcomm.com/company/product-security/bulletins/july-2020-bulletin	H-QUA-MSM8-190820/1589

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			MSM8998, Nicobar, QCA6574AU, QCM2150, QCS405, QCS605, QM215, Rennell, SA6155P, Saipan, SDA660, SDA845, SDM429, SDM429W, SDM439, SDM450, SDM630, SDM632, SDM636, SDM660, SDM670, SDM710, SDM845, SDX20, SM6150, SM7150, SM8150, SM8250, SXR1130, SXR2130 **CVE ID : CVE-2020-3688**		
Out-of-bounds Write	30-Jul-20	7.5	Out of bound write while QoS DSCP mapping due to improper input validation for data received from association response frame 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, APQ8098, MDM9150, MDM9206, MDM9207C, MDM9607, MDM9650, MSM8905, MSM8909W, MSM8917, MSM8920, MSM8937, MSM8940, MSM8953, MSM8996AU, Nicobar, QCA6174A, QCA6574AU, QCA9377, QCA9379, QCM2150, QCN7605, QCS405,	https://www.qualcomm.com/company/product-security/bulletins/july-2020-bulletin	H-QUA-MSM8-190820/1590

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			QCS605, QM215, SA6155P, Saipan, SC8180X, SDA845, SDM429, SDM429W, SDM439, SDM450, SDM630, SDM632, SDM636, SDM660, SDM845, SDX20, SDX55, SM8150, SM8250, SXR2130 **CVE ID : CVE-2020-3698**		
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	30-Jul-20	7.5	Possible out of bound access while processing assoc response from host due to improper length check before copying into buffer 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, Nicobar, QCA6174A, QCA6574AU, QCA9377, QCA9379, QCM2150, QCN7605, QCS405, QCS605, QM215, SA6155P, Saipan, SC8180X, SDA845, SDM429, SDM429W, SDM439, SDM450,	https://www.qualcomm.com/company/product-security/bulletins/july-2020-bulletin	H-QUA-MSM8-190820/1591

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			SDM630, SDM632, SDM636, SDM660, SDM845, SDX20, SDX55, SM6150, SM7150, SM8150, SM8250, SXR2130 **CVE ID : CVE-2020-3699**		
msm8996					
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	30-Jul-20	7.5	Possible buffer overflow while parsing mp4 clip with corrupted sample atoms due to improper validation of index in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables in APQ8009, APQ8017, APQ8053, APQ8096AU, APQ8098, Kamorta, MDM9206, MDM9207C, MDM9607, MSM8905, MSM8909W, MSM8917, MSM8920, MSM8937, MSM8940, MSM8953, MSM8996, MSM8996AU, MSM8998, Nicobar, QCA6574AU, QCM2150, QCS405, QCS605, QM215, Rennell, SA6155P, Saipan, SDA660, SDA845, SDM429, SDM429W, SDM439, SDM450, SDM630, SDM632, SDM636, SDM660, SDM670, SDM710, SDM845, SDX20,	https://www.qualcomm.com/company/product-security/bulletins/july-2020-bulletin	H-QUA-MSM8-190820/1592

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			SM6150, SM7150, SM8150, SM8250, SXR1130, SXR2130 **CVE ID : CVE-2020-3688**		
sdm450					
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	30-Jul-20	7.5	Possible buffer overflow while parsing mp4 clip with corrupted sample atoms due to improper validation of index in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables in APQ8009, APQ8017, APQ8053, APQ8096AU, APQ8098, Kamorta, MDM9206, MDM9207C, MDM9607, MSM8905, MSM8909W, MSM8917, MSM8920, MSM8937, MSM8940, MSM8953, MSM8996, MSM8996AU, MSM8998, Nicobar, QCA6574AU, QCM2150, QCS405, QCS605, QM215, Rennell, SA6155P, Saipan, SDA660, SDA845, SDM429, SDM429W, SDM439, SDM450, SDM630, SDM632, SDM636, SDM660, SDM670, SDM710, SDM845, SDX20, SM6150, SM7150, SM8150, SM8250, SXR1130, SXR2130	https://www.qualcomm.com/company/product-security/bulletins/july-2020-bulletin	H-QUA-SDM4-190820/1593

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2020-3688		
Out-of-bounds Write	30-Jul-20	7.5	Out of bound write while QoS DSCP mapping due to improper input validation for data received from association response frame 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, APQ8098, MDM9150, MDM9206, MDM9207C, MDM9607, MDM9650, MSM8905, MSM8909W, MSM8917, MSM8920, MSM8937, MSM8940, MSM8953, MSM8996AU, Nicobar, QCA6174A, QCA6574AU, QCA9377, QCA9379, QCM2150, QCN7605, QCS405, QCS605, QM215, SA6155P, Saipan, SC8180X, SDA845, SDM429, SDM429W, SDM439, SDM450, SDM630, SDM632, SDM636, SDM660, SDM845, SDX20, SDX55, SM8150, SM8250, SXR2130 **CVE ID : CVE-2020-3698**	https://www.qualcomm.com/company/product-security/bulletins/july-2020-bulletin	H-QUA-SDM4-190820/1594
Buffer Copy without	30-Jul-20	7.5	Possible out of bound access while processing	https://www.qualcomm.	H-QUA-SDM4-

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Checking Size of Input ('Classic Buffer Overflow')			assoc response from host due to improper length check before copying into buffer 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, Nicobar, QCA6174A, QCA6574AU, QCA9377, QCA9379, QCM2150, QCN7605, QCS405, QCS605, QM215, SA6155P, Saipan, SC8180X, SDA845, SDM429, SDM429W, SDM439, SDM450, SDM630, SDM632, SDM636, SDM660, SDM845, SDX20, SDX55, SM6150, SM7150, SM8150, SM8250, SXR2130 **CVE ID : CVE-2020-3699**	com/company/product-security/bulletins/july-2020-bulletin	190820/1595
sm8250					
Use After Free	30-Jul-20	7.5	Use-after-free issue could occur due to dangling pointer when generating a	https://www.qualcomm.com/compan	H-QUA-SM82-190820/1596

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			frame buffer in OpenGL ES in Snapdragon Compute, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music in APQ8009, Nicobar, QCM2150, QCS405, Saipan, SDM845, SM8150, SM8250, SXR2130 **CVE ID : CVE-2020-3671**	y/product-security/bulletins/july-2020-bulletin	
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	30-Jul-20	7.5	Possible buffer overflow while parsing mp4 clip with corrupted sample atoms due to improper validation of index in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables in APQ8009, APQ8017, APQ8053, APQ8096AU, APQ8098, Kamorta, MDM9206, MDM9207C, MDM9607, MSM8905, MSM8909W, MSM8917, MSM8920, MSM8937, MSM8940, MSM8953, MSM8996, MSM8996AU, MSM8998, Nicobar, QCA6574AU, QCM2150, QCS405, QCS605, QM215, Rennell, SA6155P, Saipan, SDA660, SDA845, SDM429, SDM429W, SDM439, SDM450, SDM630, SDM632, SDM636,	https://www.qualcomm.com/company/product-security/bulletins/july-2020-bulletin	H-QUA-SM82-190820/1597

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			SDM660, SDM670, SDM710, SDM845, SDX20, SM6150, SM7150, SM8150, SM8250, SXR1130, SXR2130 **CVE ID : CVE-2020-3688**		
Out-of-bounds Write	30-Jul-20	7.5	Out of bound write while QoS DSCP mapping due to improper input validation for data received from association response frame 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, APQ8098, MDM9150, MDM9206, MDM9207C, MDM9607, MDM9650, MSM8905, MSM8909W, MSM8917, MSM8920, MSM8937, MSM8940, MSM8953, MSM8996AU, Nicobar, QCA6174A, QCA6574AU, QCA9377, QCA9379, QCM2150, QCN7605, QCS405, QCS605, QM215, SA6155P, Saipan, SC8180X, SDA845, SDM429, SDM429W, SDM439, SDM450, SDM630, SDM632, SDM636, SDM660, SDM845, SDX20, SDX55, SM8150, SM8250,	https://www.qualcomm.com/company/product-security/bulletins/july-2020-bulletin	H-QUA-SM82-190820/1598

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			SXR2130 **CVE ID : CVE-2020-3698**		
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	30-Jul-20	7.5	Possible out of bound access while processing assoc response from host due to improper length check before copying into buffer 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, Nicobar, QCA6174A, QCA6574AU, QCA9377, QCA9379, QCM2150, QCN7605, QCS405, QCS605, QM215, SA6155P, Saipan, SC8180X, SDA845, SDM429, SDM429W, SDM439, SDM450, SDM630, SDM632, SDM636, SDM660, SDM845, SDX20, SDX55, SM6150, SM7150, SM8150, SM8250, SXR2130 **CVE ID : CVE-2020-3699**	https://www.qualcomm.com/company/product-security/bulletins/july-2020-bulletin	H-QUA-SM82-190820/1599

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Out-of-bounds Read	30-Jul-20	5	Possible out of bounds read due to a missing bounds check and could lead to local information disclosure in the wifi driver with no additional execution privileges needed in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking in APQ8053, APQ8096AU, IPQ4019, IPQ8064, IPQ8074, MDM9607, MSM8909W, MSM8996AU, QCA6574AU, QCA9531, QCA9558, QCA9980, SC8180X, SDM439, SDX55, SM8150, SM8250, SXR2130 **CVE ID : CVE-2020-3700**	https://www.qualcomm.com/company/product-security/bulletins/july-2020-bulletin	H-QUA-SM82-190820/1600
Use After Free	30-Jul-20	4.6	Use after free issue while processing error notification from camx driver due to not properly releasing the sequence data in Snapdragon Mobile in Saipan, SM8250, SXR2130 **CVE ID : CVE-2020-3701**	https://www.qualcomm.com/company/product-security/bulletins/july-2020-bulletin	H-QUA-SM82-190820/1601
sxr2130					
Use After Free	30-Jul-20	7.5	Use-after-free issue could occur due to dangling pointer when generating a	https://www.qualcomm.com/compan	H-QUA-SXR2-190820/1602

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			frame buffer in OpenGL ES in Snapdragon Compute, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music in APQ8009, Nicobar, QCM2150, QCS405, Saipan, SDM845, SM8150, SM8250, SXR2130 **CVE ID : CVE-2020-3671**	y/product-security/bulletins/july-2020-bulletin	
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	30-Jul-20	7.5	Possible buffer overflow while parsing mp4 clip with corrupted sample atoms due to improper validation of index in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables in APQ8009, APQ8017, APQ8053, APQ8096AU, APQ8098, Kamorta, MDM9206, MDM9207C, MDM9607, MSM8905, MSM8909W, MSM8917, MSM8920, MSM8937, MSM8940, MSM8953, MSM8996, MSM8996AU, MSM8998, Nicobar, QCA6574AU, QCM2150, QCS405, QCS605, QM215, Rennell, SA6155P, Saipan, SDA660, SDA845, SDM429, SDM429W, SDM439, SDM450, SDM630, SDM632, SDM636,	https://www.qualcomm.com/company/product-security/bulletins/july-2020-bulletin	H-QUA-SXR2-190820/1603

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			SDM660, SDM670, SDM710, SDM845, SDX20, SM6150, SM7150, SM8150, SM8250, SXR1130, SXR2130 **CVE ID : CVE-2020-3688**		
Out-of-bounds Write	30-Jul-20	7.5	Out of bound write while QoS DSCP mapping due to improper input validation for data received from association response frame 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, APQ8098, MDM9150, MDM9206, MDM9207C, MDM9607, MDM9650, MSM8905, MSM8909W, MSM8917, MSM8920, MSM8937, MSM8940, MSM8953, MSM8996AU, Nicobar, QCA6174A, QCA6574AU, QCA9377, QCA9379, QCM2150, QCN7605, QCS405, QCS605, QM215, SA6155P, Saipan, SC8180X, SDA845, SDM429, SDM429W, SDM439, SDM450, SDM630, SDM632, SDM636, SDM660, SDM845, SDX20, SDX55, SM8150, SM8250,	https://www.qualcomm.com/company/product-security/bulletins/july-2020-bulletin	H-QUA-SXR2-190820/1604

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			SXR2130 **CVE ID : CVE-2020-3698**		
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	30-Jul-20	7.5	Possible out of bound access while processing assoc response from host due to improper length check before copying into buffer 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, Nicobar, QCA6174A, QCA6574AU, QCA9377, QCA9379, QCM2150, QCN7605, QCS405, QCS605, QM215, SA6155P, Saipan, SC8180X, SDA845, SDM429, SDM429W, SDM439, SDM450, SDM630, SDM632, SDM636, SDM660, SDM845, SDX20, SDX55, SM6150, SM7150, SM8150, SM8250, SXR2130 **CVE ID : CVE-2020-3699**	https://www.qualcomm.com/company/product-security/bulletins/july-2020-bulletin	H-QUA-SXR2-190820/1605

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Out-of-bounds Read	30-Jul-20	5	Possible out of bounds read due to a missing bounds check and could lead to local information disclosure in the wifi driver with no additional execution privileges needed in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking in APQ8053, APQ8096AU, IPQ4019, IPQ8064, IPQ8074, MDM9607, MSM8909W, MSM8996AU, QCA6574AU, QCA9531, QCA9558, QCA9980, SC8180X, SDM439, SDX55, SM8150, SM8250, SXR2130 **CVE ID : CVE-2020-3700**	https://www.qualcomm.com/company/product-security/bulletins/july-2020-bulletin	H-QUA-SXR2-190820/1606
Use After Free	30-Jul-20	4.6	Use after free issue while processing error notification from camx driver due to not properly releasing the sequence data in Snapdragon Mobile in Saipan, SM8250, SXR2130 **CVE ID : CVE-2020-3701**	https://www.qualcomm.com/company/product-security/bulletins/july-2020-bulletin	H-QUA-SXR2-190820/1607
sa6155p					
Buffer Copy without Checking	30-Jul-20	7.5	Possible buffer overflow while parsing mp4 clip with corrupted sample	https://www.qualcomm.com/compan	H-QUA-SA61-190820/1608

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Size of Input ('Classic Buffer Overflow')			atoms due to improper validation of index in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables in APQ8009, APQ8017, APQ8053, APQ8096AU, APQ8098, Kamorta, MDM9206, MDM9207C, MDM9607, MSM8905, MSM8909W, MSM8917, MSM8920, MSM8937, MSM8940, MSM8953, MSM8996, MSM8996AU, MSM8998, Nicobar, QCA6574AU, QCM2150, QCS405, QCS605, QM215, Rennell, SA6155P, Saipan, SDA660, SDA845, SDM429, SDM429W, SDM439, SDM450, SDM630, SDM632, SDM636, SDM660, SDM670, SDM710, SDM845, SDX20, SM6150, SM7150, SM8150, SM8250, SXR1130, SXR2130 **CVE ID : CVE-2020-3688**	y/product-security/bulletins/july-2020-bulletin	
Out-of-bounds Write	30-Jul-20	7.5	Out of bound write while QoS DSCP mapping due to improper input validation for data received from association response frame in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer	https://www.qualcomm.com/company/product-security/bulletins/july-2020-	H-QUA-SA61-190820/1609

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, APQ8098, MDM9150, MDM9206, MDM9207C, MDM9607, MDM9650, MSM8905, MSM8909W, MSM8917, MSM8920, MSM8937, MSM8940, MSM8953, MSM8996AU, Nicobar, QCA6174A, QCA6574AU, QCA9377, QCA9379, QCM2150, QCN7605, QCS405, QCS605, QM215, SA6155P, Saipan, SC8180X, SDA845, SDM429, SDM429W, SDM439, SDM450, SDM630, SDM632, SDM636, SDM660, SDM845, SDX20, SDX55, SM8150, SM8250, SXR2130 **CVE ID : CVE-2020-3698**	bulletin	
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	30-Jul-20	7.5	Possible out of bound access while processing assoc response from host due to improper length check before copying into buffer in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile,	https://www.qualcomm.com/company/product-security/bulletins/july-2020-bulletin	H-QUA-SA61-190820/1610

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Snapdragon Voice & Music, Snapdragon Wearables in APQ8009, APQ8017, APQ8053, APQ8096AU, MDM9206, MDM9207C, MDM9607, MDM9640, MDM9650, MSM8905, MSM8909W, MSM8917, MSM8920, MSM8937, MSM8940, MSM8953, MSM8996AU, Nicobar, QCA6174A, QCA6574AU, QCA9377, QCA9379, QCM2150, QCN7605, QCS405, QCS605, QM215, SA6155P, Saipan, SC8180X, SDA845, SDM429, SDM429W, SDM439, SDM450, SDM630, SDM632, SDM636, SDM660, SDM845, SDX20, SDX55, SM6150, SM7150, SM8150, SM8250, SXR2130 **CVE ID : CVE-2020-3699**		
sc8180x					
Out-of-bounds Write	30-Jul-20	7.5	Out of bound write while QoS DSCP mapping due to improper input validation for data received from association response frame in Snapdragon Auto, Snapdragon Compute, Snapdragon Consumer Electronics Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music,	https://www.qualcomm.com/company/product-security/bulletins/july-2020-bulletin	H-QUA-SC81-190820/1611

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Snapdragon Wearables in APQ8009, APQ8017, APQ8053, APQ8096AU, APQ8098, MDM9150, MDM9206, MDM9207C, MDM9607, MDM9650, MSM8905, MSM8909W, MSM8917, MSM8920, MSM8937, MSM8940, MSM8953, MSM8996AU, Nicobar, QCA6174A, QCA6574AU, QCA9377, QCA9379, QCM2150, QCN7605, QCS405, QCS605, QM215, SA6155P, Saipan, SC8180X, SDA845, SDM429, SDM429W, SDM439, SDM450, SDM630, SDM632, SDM636, SDM660, SDM845, SDX20, SDX55, SM8150, SM8250, SXR2130 **CVE ID : CVE-2020-3698**		
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	30-Jul-20	7.5	Possible out of bound access while processing assoc response from host due to improper length check before copying into buffer 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,	https://www.qualcomm.com/company/product-security/bulletins/july-2020-bulletin	H-QUA-SC81-190820/1612

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			MDM9607, MDM9640, MDM9650, MSM8905, MSM8909W, MSM8917, MSM8920, MSM8937, MSM8940, MSM8953, MSM8996AU, Nicobar, QCA6174A, QCA6574AU, QCA9377, QCA9379, QCM2150, QCN7605, QCS405, QCS605, QM215, SA6155P, Saipan, SC8180X, SDA845, SDM429, SDM429W, SDM439, SDM450, SDM630, SDM632, SDM636, SDM660, SDM845, SDX20, SDX55, SM6150, SM7150, SM8150, SM8250, SXR2130 **CVE ID : CVE-2020-3699**		
Out-of-bounds Read	30-Jul-20	5	Possible out of bounds read due to a missing bounds check and could lead to local information disclosure in the wifi driver with no additional execution privileges needed in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking in APQ8053, APQ8096AU, IPQ4019, IPQ8064, IPQ8074,	https://www.qualcomm.com/company/product-security/bulletins/july-2020-bulletin	H-QUA-SC81-190820/1613

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			MDM9607, MSM8909W, MSM8996AU, QCA6574AU, QCA9531, QCA9558, QCA9980, SC8180X, SDM439, SDX55, SM8150, SM8250, SXR2130 **CVE ID : CVE-2020-3700**		
qcm2150					
Use After Free	30-Jul-20	7.5	Use-after-free issue could occur due to dangling pointer when generating a frame buffer in OpenGL ES in Snapdragon Compute, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music in APQ8009, Nicobar, QCM2150, QCS405, Saipan, SDM845, SM8150, SM8250, SXR2130 **CVE ID : CVE-2020-3671**	https://www.qualcomm.com/company/product-security/bulletins/july-2020-bulletin	H-QUA-QCM2-190820/1614
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	30-Jul-20	7.5	Possible buffer overflow while parsing mp4 clip with corrupted sample atoms due to improper validation of index in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables in APQ8009, APQ8017, APQ8053, APQ8096AU, APQ8098, Kamorta, MDM9206, MDM9207C, MDM9607, MSM8905,	https://www.qualcomm.com/company/product-security/bulletins/july-2020-bulletin	H-QUA-QCM2-190820/1615

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			MSM8909W, MSM8917, MSM8920, MSM8937, MSM8940, MSM8953, MSM8996, MSM8996AU, MSM8998, Nicobar, QCA6574AU, QCM2150, QCS405, QCS605, QM215, Rennell, SA6155P, Saipan, SDA660, SDA845, SDM429, SDM429W, SDM439, SDM450, SDM630, SDM632, SDM636, SDM660, SDM670, SDM710, SDM845, SDX20, SM6150, SM7150, SM8150, SM8250, SXR1130, SXR2130 **CVE ID : CVE-2020-3688**		
Out-of-bounds Write	30-Jul-20	7.5	Out of bound write while QoS DSCP mapping due to improper input validation for data received from association response frame 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, APQ8098, MDM9150, MDM9206, MDM9207C, MDM9607, MDM9650, MSM8905, MSM8909W, MSM8917, MSM8920, MSM8937, MSM8940, MSM8953, MSM8996AU,	https://www.qualcomm.com/company/product-security/bulletins/july-2020-bulletin	H-QUA-QCM2-190820/1616

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Nicobar, QCA6174A, QCA6574AU, QCA9377, QCA9379, QCM2150, QCN7605, QCS405, QCS605, QM215, SA6155P, Saipan, SC8180X, SDA845, SDM429, SDM429W, SDM439, SDM450, SDM630, SDM632, SDM636, SDM660, SDM845, SDX20, SDX55, SM8150, SM8250, SXR2130 **CVE ID : CVE-2020-3698**		
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	30-Jul-20	7.5	Possible out of bound access while processing assoc response from host due to improper length check before copying into buffer 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, Nicobar, QCA6174A, QCA6574AU, QCA9377, QCA9379, QCM2150, QCN7605, QCS405, QCS605, QM215,	https://www.qualcomm.com/company/product-security/bulletins/july-2020-bulletin	H-QUA-QCM2-190820/1617

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			SA6155P, Saipan, SC8180X, SDA845, SDM429, SDM429W, SDM439, SDM450, SDM630, SDM632, SDM636, SDM660, SDM845, SDX20, SDX55, SM6150, SM7150, SM8150, SM8250, SXR2130 **CVE ID : CVE-2020-3699**		
sdx55					
Out-of-bounds Write	30-Jul-20	7.5	Out of bound write while QoS DSCP mapping due to improper input validation for data received from association response frame 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, APQ8098, MDM9150, MDM9206, MDM9207C, MDM9607, MDM9650, MSM8905, MSM8909W, MSM8917, MSM8920, MSM8937, MSM8940, MSM8953, MSM8996AU, Nicobar, QCA6174A, QCA6574AU, QCA9377, QCA9379, QCM2150, QCN7605, QCS405, QCS605, QM215, SA6155P,	https://www.qualcomm.com/company/product-security/bulletins/july-2020-bulletin	H-QUA-SDX5-190820/1618

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Saipan, SC8180X, SDA845, SDM429, SDM429W, SDM439, SDM450, SDM630, SDM632, SDM636, SDM660, SDM845, SDX20, SDX55, SM8150, SM8250, SXR2130 **CVE ID : CVE-2020-3698**		
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	30-Jul-20	7.5	Possible out of bound access while processing assoc response from host due to improper length check before copying into buffer 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, Nicobar, QCA6174A, QCA6574AU, QCA9377, QCA9379, QCM2150, QCN7605, QCS405, QCS605, QM215, SA6155P, Saipan, SC8180X, SDA845, SDM429, SDM429W, SDM439, SDM450, SDM630, SDM632,	https://www.qualcomm.com/company/product-security/bulletins/july-2020-bulletin	H-QUA-SDX5-190820/1619

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			SDM636, SDM660, SDM845, SDX20, SDX55, SM6150, SM7150, SM8150, SM8250, SXR2130 **CVE ID : CVE-2020-3699**		
Out-of-bounds Read	30-Jul-20	5	Possible out of bounds read due to a missing bounds check and could lead to local information disclosure in the wifi driver with no additional execution privileges needed in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking in APQ8053, APQ8096AU, IPQ4019, IPQ8064, IPQ8074, MDM9607, MSM8909W, MSM8996AU, QCA6574AU, QCA9531, QCA9558, QCA9980, SC8180X, SDM439, SDX55, SM8150, SM8250, SXR2130 **CVE ID : CVE-2020-3700**	https://www.qualcomm.com/company/product-security/bulletins/july-2020-bulletin	H-QUA-SDX5-190820/1620
rennell					
Buffer Copy without Checking Size of Input ('Classic Buffer	30-Jul-20	7.5	Possible buffer overflow while parsing mp4 clip with corrupted sample atoms due to improper validation of index in Snapdragon Auto,	https://www.qualcomm.com/company/product-security/bulletins/july-	H-QUA-RENN-190820/1621

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Overflow')			Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables in APQ8009, APQ8017, APQ8053, APQ8096AU, APQ8098, Kamorta, MDM9206, MDM9207C, MDM9607, MSM8905, MSM8909W, MSM8917, MSM8920, MSM8937, MSM8940, MSM8953, MSM8996, MSM8996AU, MSM8998, Nicobar, QCA6574AU, QCM2150, QCS405, QCS605, QM215, Rennell, SA6155P, Saipan, SDA660, SDA845, SDM429, SDM429W, SDM439, SDM450, SDM630, SDM632, SDM636, SDM660, SDM670, SDM710, SDM845, SDX20, SM6150, SM7150, SM8150, SM8250, SXR1130, SXR2130 **CVE ID : CVE-2020-3688**	2020-bulletin	
saipan					
Use After Free	30-Jul-20	7.5	Use-after-free issue could occur due to dangling pointer when generating a frame buffer in OpenGL ES in Snapdragon Compute, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music	https://www.qualcomm.com/company/product-security/bulletins/july-2020-bulletin	H-QUA-SAIP-190820/1622

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			in APQ8009, Nicobar, QCM2150, QCS405, Saipan, SDM845, SM8150, SM8250, SXR2130 **CVE ID : CVE-2020-3671**		
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	30-Jul-20	7.5	Possible buffer overflow while parsing mp4 clip with corrupted sample atoms due to improper validation of index in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables in APQ8009, APQ8017, APQ8053, APQ8096AU, APQ8098, Kamorta, MDM9206, MDM9207C, MDM9607, MSM8905, MSM8909W, MSM8917, MSM8920, MSM8937, MSM8940, MSM8953, MSM8996, MSM8996AU, MSM8998, Nicobar, QCA6574AU, QCM2150, QCS405, QCS605, QM215, Rennell, SA6155P, Saipan, SDA660, SDA845, SDM429, SDM429W, SDM439, SDM450, SDM630, SDM632, SDM636, SDM660, SDM670, SDM710, SDM845, SDX20, SM6150, SM7150, SM8150, SM8250, SXR1130, SXR2130	https://www.qualcomm.com/company/product-security/bulletins/july-2020-bulletin	H-QUA-SAIP-190820/1623

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2020-3688		
Out-of-bounds Write	30-Jul-20	7.5	Out of bound write while QoS DSCP mapping due to improper input validation for data received from association response frame 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, APQ8098, MDM9150, MDM9206, MDM9207C, MDM9607, MDM9650, MSM8905, MSM8909W, MSM8917, MSM8920, MSM8937, MSM8940, MSM8953, MSM8996AU, Nicobar, QCA6174A, QCA6574AU, QCA9377, QCA9379, QCM2150, QCN7605, QCS405, QCS605, QM215, SA6155P, Saipan, SC8180X, SDA845, SDM429, SDM429W, SDM439, SDM450, SDM630, SDM632, SDM636, SDM660, SDM845, SDX20, SDX55, SM8150, SM8250, SXR2130 **CVE ID : CVE-2020-3698**	https://www.qualcomm.com/company/product-security/bulletins/july-2020-bulletin	H-QUA-SAIP-190820/1624
Buffer Copy without	30-Jul-20	7.5	Possible out of bound access while processing	https://www.qualcomm.	H-QUA-SAIP-190820/1625

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Checking Size of Input ('Classic Buffer Overflow')			assoc response from host due to improper length check before copying into buffer 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, Nicobar, QCA6174A, QCA6574AU, QCA9377, QCA9379, QCM2150, QCN7605, QCS405, QCS605, QM215, SA6155P, Saipan, SC8180X, SDA845, SDM429, SDM429W, SDM439, SDM450, SDM630, SDM632, SDM636, SDM660, SDM845, SDX20, SDX55, SM6150, SM7150, SM8150, SM8250, SXR2130 **CVE ID : CVE-2020-3699**	com/company/product-security/bulletins/july-2020-bulletin	
Use After Free	30-Jul-20	4.6	Use after free issue while processing error notification from camx driver due to not properly releasing the sequence	https://www.qualcomm.com/company/product-security/bull	H-QUA-SAIP-190820/1626

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			data in Snapdragon Mobile in Saipan, SM8250, SXR2130 **CVE ID : CVE-2020-3701**	etins/july-2020-bulletin	
kamorta					
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	30-Jul-20	7.5	Possible buffer overflow while parsing mp4 clip with corrupted sample atoms due to improper validation of index in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Industrial IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables in APQ8009, APQ8017, APQ8053, APQ8096AU, APQ8098, Kamorta, MDM9206, MDM9207C, MDM9607, MSM8905, MSM8909W, MSM8917, MSM8920, MSM8937, MSM8940, MSM8953, MSM8996, MSM8996AU, MSM8998, Nicobar, QCA6574AU, QCM2150, QCS405, QCS605, QM215, Rennell, SA6155P, Saipan, SDA660, SDA845, SDM429, SDM429W, SDM439, SDM450, SDM630, SDM632, SDM636, SDM660, SDM670, SDM710, SDM845, SDX20, SM6150, SM7150, SM8150, SM8250, SXR1130, SXR2130	https://www.qualcomm.com/company/product-security/bulletins/july-2020-bulletin	H-QUA-KAMO-190820/1627

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2020-3688		
-					
Use of a Broken or Risky Cryptographic Algorithm	31-Jul-20	7.5	Authenticated and encrypted payload MMEs can be forged and remotely sent to any HPAV2 system using a jailbreak key recoverable from code. **CVE ID : CVE-2020-3681**	https://www.qualcomm.com/company/product-security/bulletins/july-2020-bulletin	H-QUA---190820/1628
qca9558					
Out-of-bounds Read	30-Jul-20	5	Possible out of bounds read due to a missing bounds check and could lead to local information disclosure in the wifi driver with no additional execution privileges needed in Snapdragon Auto, Snapdragon Compute, Snapdragon Connectivity, Snapdragon Consumer IOT, Snapdragon Mobile, Snapdragon Voice & Music, Snapdragon Wearables, Snapdragon Wired Infrastructure and Networking in APQ8053, APQ8096AU, IPQ4019, IPQ8064, IPQ8074, MDM9607, MSM8909W, MSM8996AU, QCA6574AU, QCA9531, QCA9558, QCA9980, SC8180X, SDM439, SDX55, SM8150, SM8250, SXR2130 **CVE ID : CVE-2020-3700**	https://www.qualcomm.com/company/product-security/bulletins/july-2020-bulletin	H-QUA-QCA9-190820/1629
Ruckuswireless					

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
c110					
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	28-Jul-20	4.3	An XSS issue in emfd in Ruckus Wireless Unleashed through 200.7.10.102.92 allows a remote attacker to execute JavaScript code via an unauthenticated crafted HTTP request. This affects C110, E510, H320, H510, M510, R320, R310, R500, R510 R600, R610, R710, R720, R750, T300, T301n, T301s, T310c, T310d, T310n, T310s, T610, T710, and T710s devices. **CVE ID : CVE-2020-13913**	https://support.ruckuswireless.com/security_bulletins/304	H-RUC-C110-190820/1630
Improper Input Validation	28-Jul-20	5	webs in Ruckus Wireless Unleashed through 200.7.10.102.92 allows a remote attacker to cause a denial of service (Segmentation fault) to the webserver via an unauthenticated crafted HTTP request. This affects C110, E510, H320, H510, M510, R320, R310, R500, R510 R600, R610, R710, R720, R750, T300, T301n, T301s, T310c, T310d, T310n, T310s, T610, T710, and T710s devices. **CVE ID : CVE-2020-13914**	https://support.ruckuswireless.com/security_bulletins/304	H-RUC-C110-190820/1631
Insufficiently Protected Credentials	28-Jul-20	6.4	Insecure permissions in emfd/libemf in Ruckus Wireless Unleashed through 200.7.10.102.92 allow a remote attacker to overwrite admin	https://support.ruckuswireless.com/security_bulletins/304	H-RUC-C110-190820/1632

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			credentials via an unauthenticated crafted HTTP request. This affects C110, E510, H320, H510, M510, R320, R310, R500, R510 R600, R610, R710, R720, R750, T300, T301n, T301s, T310c, T310d, T310n, T310s, T610, T710, and T710s devices. **CVE ID : CVE-2020-13915**		
Out-of-bounds Write	28-Jul-20	7.5	A stack buffer overflow in webs in Ruckus Wireless Unleashed through 200.7.10.102.92 allows a remote attacker to execute code via an unauthenticated crafted HTTP request. This affects C110, E510, H320, H510, M510, R320, R310, R500, R510 R600, R610, R710, R720, R750, T300, T301n, T301s, T310c, T310d, T310n, T310s, T610, T710, and T710s devices. **CVE ID : CVE-2020-13916**	https://support.ruckuswireless.com/security_bulletins/304	H-RUC-C110-190820/1633
Improper Neutralization of Special Elements used in an OS Command ('OS Command Injection')	28-Jul-20	7.5	rkscli in Ruckus Wireless Unleashed through 200.7.10.92 allows a remote attacker to achieve command injection and jailbreak the CLI via a crafted CLI command. This affects C110, E510, H320, H510, M510, R320, R310, R500, R510 R600, R610, R710, R720, R750, T300, T301n, T301s, T310c, T310d, T310n, T310s,	https://support.ruckuswireless.com/security_bulletins/304	H-RUC-C110-190820/1634

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			T610, T710, and T710s devices. **CVE ID : CVE-2020-13917**		
Information Exposure	28-Jul-20	5	Incorrect access control in webs in Ruckus Wireless Unleashed through 200.7.10.102.92 allows a remote attacker to leak system information (that can be used for a jailbreak) via an unauthenticated crafted HTTP request. This affects C110, E510, H320, H510, M510, R320, R310, R500, R510 R600, R610, R710, R720, R750, T300, T301n, T301s, T310c, T310d, T310n, T310s, T610, T710, and T710s devices. **CVE ID : CVE-2020-13918**	https://support.ruckuswireless.com/security_bulletins/304	H-RUC-C110-190820/1635
Improper Neutralization of Special Elements used in an OS Command ('OS Command Injection')	28-Jul-20	7.5	emfd/libemf in Ruckus Wireless Unleashed through 200.7.10.102.92 allows a remote attacker to achieve command injection via a crafted HTTP request. This affects C110, E510, H320, H510, M510, R320, R310, R500, R510 R600, R610, R710, R720, R750, T300, T301n, T301s, T310c, T310d, T310n, T310s, T610, T710, and T710s devices. **CVE ID : CVE-2020-13919**	https://support.ruckuswireless.com/security_bulletins/304	H-RUC-C110-190820/1636
e510					
Improper Neutralizatio	28-Jul-20	4.3	An XSS issue in emfd in Ruckus Wireless	https://support.ruckuswi	H-RUC-E510-190820/1637

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
n of Input During Web Page Generation ('Cross-site Scripting')			Unleashed through 200.7.10.102.92 allows a remote attacker to execute JavaScript code via an unauthenticated crafted HTTP request. This affects C110, E510, H320, H510, M510, R320, R310, R500, R510 R600, R610, R710, R720, R750, T300, T301n, T301s, T310c, T310d, T310n, T310s, T610, T710, and T710s devices. **CVE ID : CVE-2020-13913**	reless.com/security_bulletins/304	
Improper Input Validation	28-Jul-20	5	webs in Ruckus Wireless Unleashed through 200.7.10.102.92 allows a remote attacker to cause a denial of service (Segmentation fault) to the webserver via an unauthenticated crafted HTTP request. This affects C110, E510, H320, H510, M510, R320, R310, R500, R510 R600, R610, R710, R720, R750, T300, T301n, T301s, T310c, T310d, T310n, T310s, T610, T710, and T710s devices. **CVE ID : CVE-2020-13914**	https://support.ruckuswireless.com/security_bulletins/304	H-RUC-E510-190820/1638
Insufficiently Protected Credentials	28-Jul-20	6.4	Insecure permissions in emfd/libemf in Ruckus Wireless Unleashed through 200.7.10.102.92 allow a remote attacker to overwrite admin credentials via an unauthenticated crafted HTTP request. This affects	https://support.ruckuswireless.com/security_bulletins/304	H-RUC-E510-190820/1639

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			C110, E510, H320, H510, M510, R320, R310, R500, R510 R600, R610, R710, R720, R750, T300, T301n, T301s, T310c, T310d, T310n, T310s, T610, T710, and T710s devices. **CVE ID : CVE-2020-13915**		
Out-of-bounds Write	28-Jul-20	7.5	A stack buffer overflow in webs in Ruckus Wireless Unleashed through 200.7.10.102.92 allows a remote attacker to execute code via an unauthenticated crafted HTTP request. This affects C110, E510, H320, H510, M510, R320, R310, R500, R510 R600, R610, R710, R720, R750, T300, T301n, T301s, T310c, T310d, T310n, T310s, T610, T710, and T710s devices. **CVE ID : CVE-2020-13916**	https://support.ruckuswireless.com/security_bulletins/304	H-RUC-E510-190820/1640
Improper Neutralization of Special Elements used in an OS Command ('OS Command Injection')	28-Jul-20	7.5	rkscli in Ruckus Wireless Unleashed through 200.7.10.92 allows a remote attacker to achieve command injection and jailbreak the CLI via a crafted CLI command. This affects C110, E510, H320, H510, M510, R320, R310, R500, R510 R600, R610, R710, R720, R750, T300, T301n, T301s, T310c, T310d, T310n, T310s, T610, T710, and T710s devices.	https://support.ruckuswireless.com/security_bulletins/304	H-RUC-E510-190820/1641

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2020-13917		
Information Exposure	28-Jul-20	5	Incorrect access control in webs in Ruckus Wireless Unleashed through 200.7.10.102.92 allows a remote attacker to leak system information (that can be used for a jailbreak) via an unauthenticated crafted HTTP request. This affects C110, E510, H320, H510, M510, R320, R310, R500, R510 R600, R610, R710, R720, R750, T300, T301n, T301s, T310c, T310d, T310n, T310s, T610, T710, and T710s devices. **CVE ID : CVE-2020-13918**	https://support.ruckuswireless.com/security_bulletins/304	H-RUC-E510-190820/1642
Improper Neutralization of Special Elements used in an OS Command ('OS Command Injection')	28-Jul-20	7.5	emfd/libemf in Ruckus Wireless Unleashed through 200.7.10.102.92 allows a remote attacker to achieve command injection via a crafted HTTP request. This affects C110, E510, H320, H510, M510, R320, R310, R500, R510 R600, R610, R710, R720, R750, T300, T301n, T301s, T310c, T310d, T310n, T310s, T610, T710, and T710s devices. **CVE ID : CVE-2020-13919**	https://support.ruckuswireless.com/security_bulletins/304	H-RUC-E510-190820/1643
h320					
Improper Neutralization of Input During Web	28-Jul-20	4.3	An XSS issue in emfd in Ruckus Wireless Unleashed through 200.7.10.102.92 allows a	https://support.ruckuswireless.com/security_bulle	H-RUC-H320-190820/1644

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Page Generation ('Cross-site Scripting')			remote attacker to execute JavaScript code via an unauthenticated crafted HTTP request. This affects C110, E510, H320, H510, M510, R320, R310, R500, R510 R600, R610, R710, R720, R750, T300, T301n, T301s, T310c, T310d, T310n, T310s, T610, T710, and T710s devices. **CVE ID : CVE-2020-13913**	tins/304	
Improper Input Validation	28-Jul-20	5	webs in Ruckus Wireless Unleashed through 200.7.10.102.92 allows a remote attacker to cause a denial of service (Segmentation fault) to the webserver via an unauthenticated crafted HTTP request. This affects C110, E510, H320, H510, M510, R320, R310, R500, R510 R600, R610, R710, R720, R750, T300, T301n, T301s, T310c, T310d, T310n, T310s, T610, T710, and T710s devices. **CVE ID : CVE-2020-13914**	https://support.ruckuswireless.com/security_bulletins/304	H-RUC-H320-190820/1645
Insufficiently Protected Credentials	28-Jul-20	6.4	Insecure permissions in emfd/libemf in Ruckus Wireless Unleashed through 200.7.10.102.92 allow a remote attacker to overwrite admin credentials via an unauthenticated crafted HTTP request. This affects C110, E510, H320, H510, M510, R320, R310, R500,	https://support.ruckuswireless.com/security_bulletins/304	H-RUC-H320-190820/1646

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			R510 R600, R610, R710, R720, R750, T300, T301n, T301s, T310c, T310d, T310n, T310s, T610, T710, and T710s devices. **CVE ID : CVE-2020-13915**		
Out-of-bounds Write	28-Jul-20	7.5	A stack buffer overflow in webs in Ruckus Wireless Unleashed through 200.7.10.102.92 allows a remote attacker to execute code via an unauthenticated crafted HTTP request. This affects C110, E510, H320, H510, M510, R320, R310, R500, R510 R600, R610, R710, R720, R750, T300, T301n, T301s, T310c, T310d, T310n, T310s, T610, T710, and T710s devices. **CVE ID : CVE-2020-13916**	https://support.ruckuswireless.com/security_bulletins/304	H-RUC-H320-190820/1647
Improper Neutralization of Special Elements used in an OS Command ('OS Command Injection')	28-Jul-20	7.5	rkscli in Ruckus Wireless Unleashed through 200.7.10.92 allows a remote attacker to achieve command injection and jailbreak the CLI via a crafted CLI command. This affects C110, E510, H320, H510, M510, R320, R310, R500, R510 R600, R610, R710, R720, R750, T300, T301n, T301s, T310c, T310d, T310n, T310s, T610, T710, and T710s devices. **CVE ID : CVE-2020-13917**	https://support.ruckuswireless.com/security_bulletins/304	H-RUC-H320-190820/1648
Information	28-Jul-20	5	Incorrect access control in	https://supp	H-RUC-H320-

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Exposure			webs in Ruckus Wireless Unleashed through 200.7.10.102.92 allows a remote attacker to leak system information (that can be used for a jailbreak) via an unauthenticated crafted HTTP request. This affects C110, E510, H320, H510, M510, R320, R310, R500, R510 R600, R610, R710, R720, R750, T300, T301n, T301s, T310c, T310d, T310n, T310s, T610, T710, and T710s devices. **CVE ID : CVE-2020-13918**	ort.ruckuswireless.com/security_bulletins/304	190820/1649
Improper Neutralization of Special Elements used in an OS Command ('OS Command Injection')	28-Jul-20	7.5	emfd/libemf in Ruckus Wireless Unleashed through 200.7.10.102.92 allows a remote attacker to achieve command injection via a crafted HTTP request. This affects C110, E510, H320, H510, M510, R320, R310, R500, R510 R600, R610, R710, R720, R750, T300, T301n, T301s, T310c, T310d, T310n, T310s, T610, T710, and T710s devices. **CVE ID : CVE-2020-13919**	https://support.ruckuswireless.com/security_bulletins/304	H-RUC-H320-190820/1650
h510					
Improper Neutralization of Input During Web Page Generation ('Cross-site	28-Jul-20	4.3	An XSS issue in emfd in Ruckus Wireless Unleashed through 200.7.10.102.92 allows a remote attacker to execute JavaScript code via an unauthenticated crafted	https://support.ruckuswireless.com/security_bulletins/304	H-RUC-H510-190820/1651

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Scripting')			HTTP request. This affects C110, E510, H320, H510, M510, R320, R310, R500, R510 R600, R610, R710, R720, R750, T300, T301n, T301s, T310c, T310d, T310n, T310s, T610, T710, and T710s devices. **CVE ID : CVE-2020-13913**		
Improper Input Validation	28-Jul-20	5	webs in Ruckus Wireless Unleashed through 200.7.10.102.92 allows a remote attacker to cause a denial of service (Segmentation fault) to the webserver via an unauthenticated crafted HTTP request. This affects C110, E510, H320, H510, M510, R320, R310, R500, R510 R600, R610, R710, R720, R750, T300, T301n, T301s, T310c, T310d, T310n, T310s, T610, T710, and T710s devices. **CVE ID : CVE-2020-13914**	https://support.ruckuswireless.com/security_bulletins/304	H-RUC-H510-190820/1652
Insufficiently Protected Credentials	28-Jul-20	6.4	Insecure permissions in emfd/libemf in Ruckus Wireless Unleashed through 200.7.10.102.92 allow a remote attacker to overwrite admin credentials via an unauthenticated crafted HTTP request. This affects C110, E510, H320, H510, M510, R320, R310, R500, R510 R600, R610, R710, R720, R750, T300, T301n, T301s, T310c, T310d,	https://support.ruckuswireless.com/security_bulletins/304	H-RUC-H510-190820/1653

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			T310n, T310s, T610, T710, and T710s devices. **CVE ID : CVE-2020-13915**		
Out-of-bounds Write	28-Jul-20	7.5	A stack buffer overflow in webs in Ruckus Wireless Unleashed through 200.7.10.102.92 allows a remote attacker to execute code via an unauthenticated crafted HTTP request. This affects C110, E510, H320, H510, M510, R320, R310, R500, R510 R600, R610, R710, R720, R750, T300, T301n, T301s, T310c, T310d, T310n, T310s, T610, T710, and T710s devices. **CVE ID : CVE-2020-13916**	https://support.ruckuswireless.com/security_bulletins/304	H-RUC-H510-190820/1654
Improper Neutralization of Special Elements used in an OS Command ('OS Command Injection')	28-Jul-20	7.5	rkscli in Ruckus Wireless Unleashed through 200.7.10.92 allows a remote attacker to achieve command injection and jailbreak the CLI via a crafted CLI command. This affects C110, E510, H320, H510, M510, R320, R310, R500, R510 R600, R610, R710, R720, R750, T300, T301n, T301s, T310c, T310d, T310n, T310s, T610, T710, and T710s devices. **CVE ID : CVE-2020-13917**	https://support.ruckuswireless.com/security_bulletins/304	H-RUC-H510-190820/1655
Information Exposure	28-Jul-20	5	Incorrect access control in webs in Ruckus Wireless Unleashed through 200.7.10.102.92 allows a	https://support.ruckuswireless.com/security_bulle	H-RUC-H510-190820/1656

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			remote attacker to leak system information (that can be used for a jailbreak) via an unauthenticated crafted HTTP request. This affects C110, E510, H320, H510, M510, R320, R310, R500, R510 R600, R610, R710, R720, R750, T300, T301n, T301s, T310c, T310d, T310n, T310s, T610, T710, and T710s devices. **CVE ID : CVE-2020-13918**	tins/304	
Improper Neutralization of Special Elements used in an OS Command ('OS Command Injection')	28-Jul-20	7.5	emfd/libemf in Ruckus Wireless Unleashed through 200.7.10.102.92 allows a remote attacker to achieve command injection via a crafted HTTP request. This affects C110, E510, H320, H510, M510, R320, R310, R500, R510 R600, R610, R710, R720, R750, T300, T301n, T301s, T310c, T310d, T310n, T310s, T610, T710, and T710s devices. **CVE ID : CVE-2020-13919**	https://support.ruckuswireless.com/security_bulletins/304	H-RUC-H510-190820/1657
m510					
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	28-Jul-20	4.3	An XSS issue in emfd in Ruckus Wireless Unleashed through 200.7.10.102.92 allows a remote attacker to execute JavaScript code via an unauthenticated crafted HTTP request. This affects C110, E510, H320, H510, M510, R320, R310, R500,	https://support.ruckuswireless.com/security_bulletins/304	H-RUC-M510-190820/1658

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			R510 R600, R610, R710, R720, R750, T300, T301n, T301s, T310c, T310d, T310n, T310s, T610, T710, and T710s devices. **CVE ID : CVE-2020-13913**		
Improper Input Validation	28-Jul-20	5	webs in Ruckus Wireless Unleashed through 200.7.10.102.92 allows a remote attacker to cause a denial of service (Segmentation fault) to the webserver via an unauthenticated crafted HTTP request. This affects C110, E510, H320, H510, M510, R320, R310, R500, R510 R600, R610, R710, R720, R750, T300, T301n, T301s, T310c, T310d, T310n, T310s, T610, T710, and T710s devices. **CVE ID : CVE-2020-13914**	https://support.ruckuswireless.com/security_bulletins/304	H-RUC-M510-190820/1659
Insufficiently Protected Credentials	28-Jul-20	6.4	Insecure permissions in emfd/libemf in Ruckus Wireless Unleashed through 200.7.10.102.92 allow a remote attacker to overwrite admin credentials via an unauthenticated crafted HTTP request. This affects C110, E510, H320, H510, M510, R320, R310, R500, R510 R600, R610, R710, R720, R750, T300, T301n, T301s, T310c, T310d, T310n, T310s, T610, T710, and T710s devices.	https://support.ruckuswireless.com/security_bulletins/304	H-RUC-M510-190820/1660

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2020-13915		
Out-of-bounds Write	28-Jul-20	7.5	A stack buffer overflow in webs in Ruckus Wireless Unleashed through 200.7.10.102.92 allows a remote attacker to execute code via an unauthenticated crafted HTTP request. This affects C110, E510, H320, H510, M510, R320, R310, R500, R510 R600, R610, R710, R720, R750, T300, T301n, T301s, T310c, T310d, T310n, T310s, T610, T710, and T710s devices. **CVE ID : CVE-2020-13916**	https://support.ruckuswireless.com/security_bulletins/304	H-RUC-M510-190820/1661
Improper Neutralization of Special Elements used in an OS Command ('OS Command Injection')	28-Jul-20	7.5	rkscli in Ruckus Wireless Unleashed through 200.7.10.92 allows a remote attacker to achieve command injection and jailbreak the CLI via a crafted CLI command. This affects C110, E510, H320, H510, M510, R320, R310, R500, R510 R600, R610, R710, R720, R750, T300, T301n, T301s, T310c, T310d, T310n, T310s, T610, T710, and T710s devices. **CVE ID : CVE-2020-13917**	https://support.ruckuswireless.com/security_bulletins/304	H-RUC-M510-190820/1662
Information Exposure	28-Jul-20	5	Incorrect access control in webs in Ruckus Wireless Unleashed through 200.7.10.102.92 allows a remote attacker to leak system information (that can be used for a jailbreak)	https://support.ruckuswireless.com/security_bulletins/304	H-RUC-M510-190820/1663

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			via an unauthenticated crafted HTTP request. This affects C110, E510, H320, H510, M510, R320, R310, R500, R510 R600, R610, R710, R720, R750, T300, T301n, T301s, T310c, T310d, T310n, T310s, T610, T710, and T710s devices. **CVE ID : CVE-2020-13918**		
Improper Neutralization of Special Elements used in an OS Command ('OS Command Injection')	28-Jul-20	7.5	emfd/libemf in Ruckus Wireless Unleashed through 200.7.10.102.92 allows a remote attacker to achieve command injection via a crafted HTTP request. This affects C110, E510, H320, H510, M510, R320, R310, R500, R510 R600, R610, R710, R720, R750, T300, T301n, T301s, T310c, T310d, T310n, T310s, T610, T710, and T710s devices. **CVE ID : CVE-2020-13919**	https://support.ruckuswireless.com/security_bulletins/304	H-RUC-M510-190820/1664
r320					
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	28-Jul-20	4.3	An XSS issue in emfd in Ruckus Wireless Unleashed through 200.7.10.102.92 allows a remote attacker to execute JavaScript code via an unauthenticated crafted HTTP request. This affects C110, E510, H320, H510, M510, R320, R310, R500, R510 R600, R610, R710, R720, R750, T300, T301n, T301s, T310c, T310d,	https://support.ruckuswireless.com/security_bulletins/304	H-RUC-R320-190820/1665

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			T310n, T310s, T610, T710, and T710s devices. **CVE ID : CVE-2020-13913**		
Improper Input Validation	28-Jul-20	5	webs in Ruckus Wireless Unleashed through 200.7.10.102.92 allows a remote attacker to cause a denial of service (Segmentation fault) to the webserver via an unauthenticated crafted HTTP request. This affects C110, E510, H320, H510, M510, R320, R310, R500, R510 R600, R610, R710, R720, R750, T300, T301n, T301s, T310c, T310d, T310n, T310s, T610, T710, and T710s devices. **CVE ID : CVE-2020-13914**	https://support.ruckuswireless.com/security_bulletins/304	H-RUC-R320-190820/1666
Insufficiently Protected Credentials	28-Jul-20	6.4	Insecure permissions in emfd/libemf in Ruckus Wireless Unleashed through 200.7.10.102.92 allow a remote attacker to overwrite admin credentials via an unauthenticated crafted HTTP request. This affects C110, E510, H320, H510, M510, R320, R310, R500, R510 R600, R610, R710, R720, R750, T300, T301n, T301s, T310c, T310d, T310n, T310s, T610, T710, and T710s devices. **CVE ID : CVE-2020-13915**	https://support.ruckuswireless.com/security_bulletins/304	H-RUC-R320-190820/1667
Out-of-bounds	28-Jul-20	7.5	A stack buffer overflow in webs in Ruckus Wireless	https://support.ruckuswi	H-RUC-R320-190820/1668

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Write			Unleashed through 200.7.10.102.92 allows a remote attacker to execute code via an unauthenticated crafted HTTP request. This affects C110, E510, H320, H510, M510, R320, R310, R500, R510 R600, R610, R710, R720, R750, T300, T301n, T301s, T310c, T310d, T310n, T310s, T610, T710, and T710s devices. **CVE ID : CVE-2020-13916**	reless.com/security_bulletins/304	
Improper Neutralization of Special Elements used in an OS Command ('OS Command Injection')	28-Jul-20	7.5	rkscli in Ruckus Wireless Unleashed through 200.7.10.92 allows a remote attacker to achieve command injection and jailbreak the CLI via a crafted CLI command. This affects C110, E510, H320, H510, M510, R320, R310, R500, R510 R600, R610, R710, R720, R750, T300, T301n, T301s, T310c, T310d, T310n, T310s, T610, T710, and T710s devices. **CVE ID : CVE-2020-13917**	https://support.ruckuswireless.com/security_bulletins/304	H-RUC-R320-190820/1669
Information Exposure	28-Jul-20	5	Incorrect access control in webs in Ruckus Wireless Unleashed through 200.7.10.102.92 allows a remote attacker to leak system information (that can be used for a jailbreak) via an unauthenticated crafted HTTP request. This affects C110, E510, H320,	https://support.ruckuswireless.com/security_bulletins/304	H-RUC-R320-190820/1670

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			H510, M510, R320, R310, R500, R510 R600, R610, R710, R720, R750, T300, T301n, T301s, T310c, T310d, T310n, T310s, T610, T710, and T710s devices. **CVE ID : CVE-2020-13918**		
Improper Neutralization of Special Elements used in an OS Command ('OS Command Injection')	28-Jul-20	7.5	emfd/libemf in Ruckus Wireless Unleashed through 200.7.10.102.92 allows a remote attacker to achieve command injection via a crafted HTTP request. This affects C110, E510, H320, H510, M510, R320, R310, R500, R510 R600, R610, R710, R720, R750, T300, T301n, T301s, T310c, T310d, T310n, T310s, T610, T710, and T710s devices. **CVE ID : CVE-2020-13919**	https://support.ruckuswireless.com/security_bulletins/304	H-RUC-R320-190820/1671
r500					
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	28-Jul-20	4.3	An XSS issue in emfd in Ruckus Wireless Unleashed through 200.7.10.102.92 allows a remote attacker to execute JavaScript code via an unauthenticated crafted HTTP request. This affects C110, E510, H320, H510, M510, R320, R310, R500, R510 R600, R610, R710, R720, R750, T300, T301n, T301s, T310c, T310d, T310n, T310s, T610, T710, and T710s devices.	https://support.ruckuswireless.com/security_bulletins/304	H-RUC-R500-190820/1672

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2020-13913		
Improper Input Validation	28-Jul-20	5	webs in Ruckus Wireless Unleashed through 200.7.10.102.92 allows a remote attacker to cause a denial of service (Segmentation fault) to the webserver via an unauthenticated crafted HTTP request. This affects C110, E510, H320, H510, M510, R320, R310, R500, R510 R600, R610, R710, R720, R750, T300, T301n, T301s, T310c, T310d, T310n, T310s, T610, T710, and T710s devices. **CVE ID : CVE-2020-13914**	https://support.ruckuswireless.com/security_bulletins/304	H-RUC-R500-190820/1673
Insufficiently Protected Credentials	28-Jul-20	6.4	Insecure permissions in emfd/libemf in Ruckus Wireless Unleashed through 200.7.10.102.92 allow a remote attacker to overwrite admin credentials via an unauthenticated crafted HTTP request. This affects C110, E510, H320, H510, M510, R320, R310, R500, R510 R600, R610, R710, R720, R750, T300, T301n, T301s, T310c, T310d, T310n, T310s, T610, T710, and T710s devices. **CVE ID : CVE-2020-13915**	https://support.ruckuswireless.com/security_bulletins/304	H-RUC-R500-190820/1674
Out-of-bounds Write	28-Jul-20	7.5	A stack buffer overflow in webs in Ruckus Wireless Unleashed through 200.7.10.102.92 allows a remote attacker to execute	https://support.ruckuswireless.com/security_bulle	H-RUC-R500-190820/1675

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			code via an unauthenticated crafted HTTP request. This affects C110, E510, H320, H510, M510, R320, R310, R500, R510 R600, R610, R710, R720, R750, T300, T301n, T301s, T310c, T310d, T310n, T310s, T610, T710, and T710s devices. **CVE ID : CVE-2020-13916**	tins/304	
Improper Neutralization of Special Elements used in an OS Command ('OS Command Injection')	28-Jul-20	7.5	rkscli in Ruckus Wireless Unleashed through 200.7.10.92 allows a remote attacker to achieve command injection and jailbreak the CLI via a crafted CLI command. This affects C110, E510, H320, H510, M510, R320, R310, R500, R510 R600, R610, R710, R720, R750, T300, T301n, T301s, T310c, T310d, T310n, T310s, T610, T710, and T710s devices. **CVE ID : CVE-2020-13917**	https://support.ruckuswireless.com/security_bulletins/304	H-RUC-R500-190820/1676
Information Exposure	28-Jul-20	5	Incorrect access control in webs in Ruckus Wireless Unleashed through 200.7.10.102.92 allows a remote attacker to leak system information (that can be used for a jailbreak) via an unauthenticated crafted HTTP request. This affects C110, E510, H320, H510, M510, R320, R310, R500, R510 R600, R610, R710, R720, R750, T300,	https://support.ruckuswireless.com/security_bulletins/304	H-RUC-R500-190820/1677

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			T301n, T301s, T310c, T310d, T310n, T310s, T610, T710, and T710s devices. **CVE ID : CVE-2020-13918**		
Improper Neutralization of Special Elements used in an OS Command ('OS Command Injection')	28-Jul-20	7.5	emfd/libemf in Ruckus Wireless Unleashed through 200.7.10.102.92 allows a remote attacker to achieve command injection via a crafted HTTP request. This affects C110, E510, H320, H510, M510, R320, R310, R500, R510 R600, R610, R710, R720, R750, T300, T301n, T301s, T310c, T310d, T310n, T310s, T610, T710, and T710s devices. **CVE ID : CVE-2020-13919**	https://support.ruckuswireless.com/security_bulletins/304	H-RUC-R500-190820/1678
r510					
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	28-Jul-20	4.3	An XSS issue in emfd in Ruckus Wireless Unleashed through 200.7.10.102.92 allows a remote attacker to execute JavaScript code via an unauthenticated crafted HTTP request. This affects C110, E510, H320, H510, M510, R320, R310, R500, R510 R600, R610, R710, R720, R750, T300, T301n, T301s, T310c, T310d, T310n, T310s, T610, T710, and T710s devices. **CVE ID : CVE-2020-13913**	https://support.ruckuswireless.com/security_bulletins/304	H-RUC-R510-190820/1679
Improper Input	28-Jul-20	5	webs in Ruckus Wireless Unleashed through	https://support.ruckuswi	H-RUC-R510-190820/1680

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Validation			200.7.10.102.92 allows a remote attacker to cause a denial of service (Segmentation fault) to the webserver via an unauthenticated crafted HTTP request. This affects C110, E510, H320, H510, M510, R320, R310, R500, R510 R600, R610, R710, R720, R750, T300, T301n, T301s, T310c, T310d, T310n, T310s, T610, T710, and T710s devices. **CVE ID : CVE-2020-13914**	reless.com/security_bulletins/304	
Insufficiently Protected Credentials	28-Jul-20	6.4	Insecure permissions in emfd/libemf in Ruckus Wireless Unleashed through 200.7.10.102.92 allow a remote attacker to overwrite admin credentials via an unauthenticated crafted HTTP request. This affects C110, E510, H320, H510, M510, R320, R310, R500, R510 R600, R610, R710, R720, R750, T300, T301n, T301s, T310c, T310d, T310n, T310s, T610, T710, and T710s devices. **CVE ID : CVE-2020-13915**	https://support.ruckuswireless.com/security_bulletins/304	H-RUC-R510-190820/1681
Out-of-bounds Write	28-Jul-20	7.5	A stack buffer overflow in webs in Ruckus Wireless Unleashed through 200.7.10.102.92 allows a remote attacker to execute code via an unauthenticated crafted HTTP request. This affects	https://support.ruckuswireless.com/security_bulletins/304	H-RUC-R510-190820/1682

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			C110, E510, H320, H510, M510, R320, R310, R500, R510 R600, R610, R710, R720, R750, T300, T301n, T301s, T310c, T310d, T310n, T310s, T610, T710, and T710s devices. **CVE ID : CVE-2020-13916**		
Improper Neutralization of Special Elements used in an OS Command ('OS Command Injection')	28-Jul-20	7.5	rkscli in Ruckus Wireless Unleashed through 200.7.10.92 allows a remote attacker to achieve command injection and jailbreak the CLI via a crafted CLI command. This affects C110, E510, H320, H510, M510, R320, R310, R500, R510 R600, R610, R710, R720, R750, T300, T301n, T301s, T310c, T310d, T310n, T310s, T610, T710, and T710s devices. **CVE ID : CVE-2020-13917**	https://support.ruckuswireless.com/security_bulletins/304	H-RUC-R510-190820/1683
Information Exposure	28-Jul-20	5	Incorrect access control in webs in Ruckus Wireless Unleashed through 200.7.10.102.92 allows a remote attacker to leak system information (that can be used for a jailbreak) via an unauthenticated crafted HTTP request. This affects C110, E510, H320, H510, M510, R320, R310, R500, R510 R600, R610, R710, R720, R750, T300, T301n, T301s, T310c, T310d, T310n, T310s, T610, T710, and T710s	https://support.ruckuswireless.com/security_bulletins/304	H-RUC-R510-190820/1684

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			devices. **CVE ID : CVE-2020-13918**		
Improper Neutralization of Special Elements used in an OS Command ('OS Command Injection')	28-Jul-20	7.5	emfd/libemf in Ruckus Wireless Unleashed through 200.7.10.102.92 allows a remote attacker to achieve command injection via a crafted HTTP request. This affects C110, E510, H320, H510, M510, R320, R310, R500, R510 R600, R610, R710, R720, R750, T300, T301n, T301s, T310c, T310d, T310n, T310s, T610, T710, and T710s devices. **CVE ID : CVE-2020-13919**	https://support.ruckuswireless.com/security_bulletins/304	H-RUC-R510-190820/1685
r600					
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	28-Jul-20	4.3	An XSS issue in emfd in Ruckus Wireless Unleashed through 200.7.10.102.92 allows a remote attacker to execute JavaScript code via an unauthenticated crafted HTTP request. This affects C110, E510, H320, H510, M510, R320, R310, R500, R510 R600, R610, R710, R720, R750, T300, T301n, T301s, T310c, T310d, T310n, T310s, T610, T710, and T710s devices. **CVE ID : CVE-2020-13913**	https://support.ruckuswireless.com/security_bulletins/304	H-RUC-R600-190820/1686
Improper Input Validation	28-Jul-20	5	webs in Ruckus Wireless Unleashed through 200.7.10.102.92 allows a remote attacker to cause a denial of service	https://support.ruckuswireless.com/security_bulletins/304	H-RUC-R600-190820/1687

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			(Segmentation fault) to the webserver via an unauthenticated crafted HTTP request. This affects C110, E510, H320, H510, M510, R320, R310, R500, R510 R600, R610, R710, R720, R750, T300, T301n, T301s, T310c, T310d, T310n, T310s, T610, T710, and T710s devices. **CVE ID : CVE-2020-13914**		
Insufficiently Protected Credentials	28-Jul-20	6.4	Insecure permissions in emfd/libemf in Ruckus Wireless Unleashed through 200.7.10.102.92 allow a remote attacker to overwrite admin credentials via an unauthenticated crafted HTTP request. This affects C110, E510, H320, H510, M510, R320, R310, R500, R510 R600, R610, R710, R720, R750, T300, T301n, T301s, T310c, T310d, T310n, T310s, T610, T710, and T710s devices. **CVE ID : CVE-2020-13915**	https://support.ruckuswireless.com/security_bulletins/304	H-RUC-R600-190820/1688
Out-of-bounds Write	28-Jul-20	7.5	A stack buffer overflow in webs in Ruckus Wireless Unleashed through 200.7.10.102.92 allows a remote attacker to execute code via an unauthenticated crafted HTTP request. This affects C110, E510, H320, H510, M510, R320, R310, R500, R510 R600, R610, R710,	https://support.ruckuswireless.com/security_bulletins/304	H-RUC-R600-190820/1689

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			R720, R750, T300, T301n, T301s, T310c, T310d, T310n, T310s, T610, T710, and T710s devices. **CVE ID : CVE-2020-13916**		
Improper Neutralization of Special Elements used in an OS Command ('OS Command Injection')	28-Jul-20	7.5	rkscli in Ruckus Wireless Unleashed through 200.7.10.92 allows a remote attacker to achieve command injection and jailbreak the CLI via a crafted CLI command. This affects C110, E510, H320, H510, M510, R320, R310, R500, R510 R600, R610, R710, R720, R750, T300, T301n, T301s, T310c, T310d, T310n, T310s, T610, T710, and T710s devices. **CVE ID : CVE-2020-13917**	https://support.ruckuswireless.com/security_bulletins/304	H-RUC-R600-190820/1690
Information Exposure	28-Jul-20	5	Incorrect access control in webs in Ruckus Wireless Unleashed through 200.7.10.102.92 allows a remote attacker to leak system information (that can be used for a jailbreak) via an unauthenticated crafted HTTP request. This affects C110, E510, H320, H510, M510, R320, R310, R500, R510 R600, R610, R710, R720, R750, T300, T301n, T301s, T310c, T310d, T310n, T310s, T610, T710, and T710s devices. **CVE ID : CVE-2020-13918**	https://support.ruckuswireless.com/security_bulletins/304	H-RUC-R600-190820/1691

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Improper Neutralization of Special Elements used in an OS Command ('OS Command Injection')	28-Jul-20	7.5	emfd/libemf in Ruckus Wireless Unleashed through 200.7.10.102.92 allows a remote attacker to achieve command injection via a crafted HTTP request. This affects C110, E510, H320, H510, M510, R320, R310, R500, R510 R600, R610, R710, R720, R750, T300, T301n, T301s, T310c, T310d, T310n, T310s, T610, T710, and T710s devices. **CVE ID : CVE-2020-13919**	https://support.ruckuswireless.com/security_bulletins/304	H-RUC-R600-190820/1692
r610					
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	28-Jul-20	4.3	An XSS issue in emfd in Ruckus Wireless Unleashed through 200.7.10.102.92 allows a remote attacker to execute JavaScript code via an unauthenticated crafted HTTP request. This affects C110, E510, H320, H510, M510, R320, R310, R500, R510 R600, R610, R710, R720, R750, T300, T301n, T301s, T310c, T310d, T310n, T310s, T610, T710, and T710s devices. **CVE ID : CVE-2020-13913**	https://support.ruckuswireless.com/security_bulletins/304	H-RUC-R610-190820/1693
Improper Input Validation	28-Jul-20	5	webs in Ruckus Wireless Unleashed through 200.7.10.102.92 allows a remote attacker to cause a denial of service (Segmentation fault) to the webserver via an unauthenticated crafted	https://support.ruckuswireless.com/security_bulletins/304	H-RUC-R610-190820/1694

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			HTTP request. This affects C110, E510, H320, H510, M510, R320, R310, R500, R510 R600, R610, R710, R720, R750, T300, T301n, T301s, T310c, T310d, T310n, T310s, T610, T710, and T710s devices. **CVE ID : CVE-2020-13914**		
Insufficiently Protected Credentials	28-Jul-20	6.4	Insecure permissions in emfd/libemf in Ruckus Wireless Unleashed through 200.7.10.102.92 allow a remote attacker to overwrite admin credentials via an unauthenticated crafted HTTP request. This affects C110, E510, H320, H510, M510, R320, R310, R500, R510 R600, R610, R710, R720, R750, T300, T301n, T301s, T310c, T310d, T310n, T310s, T610, T710, and T710s devices. **CVE ID : CVE-2020-13915**	https://support.ruckuswireless.com/security_bulletins/304	H-RUC-R610-190820/1695
Out-of-bounds Write	28-Jul-20	7.5	A stack buffer overflow in webs in Ruckus Wireless Unleashed through 200.7.10.102.92 allows a remote attacker to execute code via an unauthenticated crafted HTTP request. This affects C110, E510, H320, H510, M510, R320, R310, R500, R510 R600, R610, R710, R720, R750, T300, T301n, T301s, T310c, T310d, T310n, T310s, T610, T710,	https://support.ruckuswireless.com/security_bulletins/304	H-RUC-R610-190820/1696

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			and T710s devices. **CVE ID : CVE-2020-13916**		
Improper Neutralization of Special Elements used in an OS Command ('OS Command Injection')	28-Jul-20	7.5	rkscli in Ruckus Wireless Unleashed through 200.7.10.92 allows a remote attacker to achieve command injection and jailbreak the CLI via a crafted CLI command. This affects C110, E510, H320, H510, M510, R320, R310, R500, R510 R600, R610, R710, R720, R750, T300, T301n, T301s, T310c, T310d, T310n, T310s, T610, T710, and T710s devices. **CVE ID : CVE-2020-13917**	https://support.ruckuswireless.com/security_bulletins/304	H-RUC-R610-190820/1697
Information Exposure	28-Jul-20	5	Incorrect access control in webs in Ruckus Wireless Unleashed through 200.7.10.102.92 allows a remote attacker to leak system information (that can be used for a jailbreak) via an unauthenticated crafted HTTP request. This affects C110, E510, H320, H510, M510, R320, R310, R500, R510 R600, R610, R710, R720, R750, T300, T301n, T301s, T310c, T310d, T310n, T310s, T610, T710, and T710s devices. **CVE ID : CVE-2020-13918**	https://support.ruckuswireless.com/security_bulletins/304	H-RUC-R610-190820/1698
Improper Neutralization of Special	28-Jul-20	7.5	emfd/libemf in Ruckus Wireless Unleashed through 200.7.10.102.92	https://support.ruckuswireless.com/s	H-RUC-R610-190820/1699

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Elements used in an OS Command ('OS Command Injection')			allows a remote attacker to achieve command injection via a crafted HTTP request. This affects C110, E510, H320, H510, M510, R320, R310, R500, R510 R600, R610, R710, R720, R750, T300, T301n, T301s, T310c, T310d, T310n, T310s, T610, T710, and T710s devices. **CVE ID : CVE-2020-13919**	ecurity_bulletins/304	
r710					
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	28-Jul-20	4.3	An XSS issue in emfd in Ruckus Wireless Unleashed through 200.7.10.102.92 allows a remote attacker to execute JavaScript code via an unauthenticated crafted HTTP request. This affects C110, E510, H320, H510, M510, R320, R310, R500, R510 R600, R610, R710, R720, R750, T300, T301n, T301s, T310c, T310d, T310n, T310s, T610, T710, and T710s devices. **CVE ID : CVE-2020-13913**	https://support.ruckuswireless.com/security_bulletins/304	H-RUC-R710-190820/1700
Improper Input Validation	28-Jul-20	5	webs in Ruckus Wireless Unleashed through 200.7.10.102.92 allows a remote attacker to cause a denial of service (Segmentation fault) to the webserver via an unauthenticated crafted HTTP request. This affects C110, E510, H320, H510, M510, R320, R310, R500,	https://support.ruckuswireless.com/security_bulletins/304	H-RUC-R710-190820/1701

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			R510 R600, R610, R710, R720, R750, T300, T301n, T301s, T310c, T310d, T310n, T310s, T610, T710, and T710s devices. **CVE ID : CVE-2020-13914**		
Insufficiently Protected Credentials	28-Jul-20	6.4	Insecure permissions in emfd/libemf in Ruckus Wireless Unleashed through 200.7.10.102.92 allow a remote attacker to overwrite admin credentials via an unauthenticated crafted HTTP request. This affects C110, E510, H320, H510, M510, R320, R310, R500, R510 R600, R610, R710, R720, R750, T300, T301n, T301s, T310c, T310d, T310n, T310s, T610, T710, and T710s devices. **CVE ID : CVE-2020-13915**	https://support.ruckuswireless.com/security_bulletins/304	H-RUC-R710-190820/1702
Out-of-bounds Write	28-Jul-20	7.5	A stack buffer overflow in webs in Ruckus Wireless Unleashed through 200.7.10.102.92 allows a remote attacker to execute code via an unauthenticated crafted HTTP request. This affects C110, E510, H320, H510, M510, R320, R310, R500, R510 R600, R610, R710, R720, R750, T300, T301n, T301s, T310c, T310d, T310n, T310s, T610, T710, and T710s devices. **CVE ID : CVE-2020-13916**	https://support.ruckuswireless.com/security_bulletins/304	H-RUC-R710-190820/1703

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Improper Neutralization of Special Elements used in an OS Command ('OS Command Injection')	28-Jul-20	7.5	rkscli in Ruckus Wireless Unleashed through 200.7.10.92 allows a remote attacker to achieve command injection and jailbreak the CLI via a crafted CLI command. This affects C110, E510, H320, H510, M510, R320, R310, R500, R510 R600, R610, R710, R720, R750, T300, T301n, T301s, T310c, T310d, T310n, T310s, T610, T710, and T710s devices. **CVE ID : CVE-2020-13917**	https://support.ruckuswireless.com/security_bulletins/304	H-RUC-R710-190820/1704
Information Exposure	28-Jul-20	5	Incorrect access control in webs in Ruckus Wireless Unleashed through 200.7.10.102.92 allows a remote attacker to leak system information (that can be used for a jailbreak) via an unauthenticated crafted HTTP request. This affects C110, E510, H320, H510, M510, R320, R310, R500, R510 R600, R610, R710, R720, R750, T300, T301n, T301s, T310c, T310d, T310n, T310s, T610, T710, and T710s devices. **CVE ID : CVE-2020-13918**	https://support.ruckuswireless.com/security_bulletins/304	H-RUC-R710-190820/1705
Improper Neutralization of Special Elements used in an OS Command	28-Jul-20	7.5	emfd/libemf in Ruckus Wireless Unleashed through 200.7.10.102.92 allows a remote attacker to achieve command injection via a crafted	https://support.ruckuswireless.com/security_bulletins/304	H-RUC-R710-190820/1706

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
('OS Command Injection')			HTTP request. This affects C110, E510, H320, H510, M510, R320, R310, R500, R510 R600, R610, R710, R720, R750, T300, T301n, T301s, T310c, T310d, T310n, T310s, T610, T710, and T710s devices. **CVE ID : CVE-2020-13919**		
r720					
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	28-Jul-20	4.3	An XSS issue in emfd in Ruckus Wireless Unleashed through 200.7.10.102.92 allows a remote attacker to execute JavaScript code via an unauthenticated crafted HTTP request. This affects C110, E510, H320, H510, M510, R320, R310, R500, R510 R600, R610, R710, R720, R750, T300, T301n, T301s, T310c, T310d, T310n, T310s, T610, T710, and T710s devices. **CVE ID : CVE-2020-13913**	https://support.ruckuswireless.com/security_bulletins/304	H-RUC-R720-190820/1707
Improper Input Validation	28-Jul-20	5	webs in Ruckus Wireless Unleashed through 200.7.10.102.92 allows a remote attacker to cause a denial of service (Segmentation fault) to the webserver via an unauthenticated crafted HTTP request. This affects C110, E510, H320, H510, M510, R320, R310, R500, R510 R600, R610, R710, R720, R750, T300, T301n, T301s, T310c, T310d,	https://support.ruckuswireless.com/security_bulletins/304	H-RUC-R720-190820/1708

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			T310n, T310s, T610, T710, and T710s devices. **CVE ID : CVE-2020-13914**		
Insufficiently Protected Credentials	28-Jul-20	6.4	Insecure permissions in emfd/libemf in Ruckus Wireless Unleashed through 200.7.10.102.92 allow a remote attacker to overwrite admin credentials via an unauthenticated crafted HTTP request. This affects C110, E510, H320, H510, M510, R320, R310, R500, R510 R600, R610, R710, R720, R750, T300, T301n, T301s, T310c, T310d, T310n, T310s, T610, T710, and T710s devices. **CVE ID : CVE-2020-13915**	https://support.ruckuswireless.com/security_bulletins/304	H-RUC-R720-190820/1709
Out-of-bounds Write	28-Jul-20	7.5	A stack buffer overflow in webs in Ruckus Wireless Unleashed through 200.7.10.102.92 allows a remote attacker to execute code via an unauthenticated crafted HTTP request. This affects C110, E510, H320, H510, M510, R320, R310, R500, R510 R600, R610, R710, R720, R750, T300, T301n, T301s, T310c, T310d, T310n, T310s, T610, T710, and T710s devices. **CVE ID : CVE-2020-13916**	https://support.ruckuswireless.com/security_bulletins/304	H-RUC-R720-190820/1710
Improper Neutralization of Special	28-Jul-20	7.5	rkscli in Ruckus Wireless Unleashed through 200.7.10.92 allows a	https://support.ruckuswireless.com/s	H-RUC-R720-190820/1711

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Elements used in an OS Command ('OS Command Injection')			remote attacker to achieve command injection and jailbreak the CLI via a crafted CLI command. This affects C110, E510, H320, H510, M510, R320, R310, R500, R510 R600, R610, R710, R720, R750, T300, T301n, T301s, T310c, T310d, T310n, T310s, T610, T710, and T710s devices. **CVE ID : CVE-2020-13917**	ecurity_bulletins/304	
Information Exposure	28-Jul-20	5	Incorrect access control in webs in Ruckus Wireless Unleashed through 200.7.10.102.92 allows a remote attacker to leak system information (that can be used for a jailbreak) via an unauthenticated crafted HTTP request. This affects C110, E510, H320, H510, M510, R320, R310, R500, R510 R600, R610, R710, R720, R750, T300, T301n, T301s, T310c, T310d, T310n, T310s, T610, T710, and T710s devices. **CVE ID : CVE-2020-13918**	https://support.ruckuswireless.com/security_bulletins/304	H-RUC-R720-190820/1712
Improper Neutralization of Special Elements used in an OS Command ('OS Command Injection')	28-Jul-20	7.5	emfd/libemf in Ruckus Wireless Unleashed through 200.7.10.102.92 allows a remote attacker to achieve command injection via a crafted HTTP request. This affects C110, E510, H320, H510, M510, R320, R310, R500,	https://support.ruckuswireless.com/security_bulletins/304	H-RUC-R720-190820/1713

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			R510 R600, R610, R710, R720, R750, T300, T301n, T301s, T310c, T310d, T310n, T310s, T610, T710, and T710s devices. **CVE ID : CVE-2020-13919**		
r750					
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	28-Jul-20	4.3	An XSS issue in emfd in Ruckus Wireless Unleashed through 200.7.10.102.92 allows a remote attacker to execute JavaScript code via an unauthenticated crafted HTTP request. This affects C110, E510, H320, H510, M510, R320, R310, R500, R510 R600, R610, R710, R720, R750, T300, T301n, T301s, T310c, T310d, T310n, T310s, T610, T710, and T710s devices. **CVE ID : CVE-2020-13913**	https://support.ruckuswireless.com/security_bulletins/304	H-RUC-R750-190820/1714
Improper Input Validation	28-Jul-20	5	webs in Ruckus Wireless Unleashed through 200.7.10.102.92 allows a remote attacker to cause a denial of service (Segmentation fault) to the webserver via an unauthenticated crafted HTTP request. This affects C110, E510, H320, H510, M510, R320, R310, R500, R510 R600, R610, R710, R720, R750, T300, T301n, T301s, T310c, T310d, T310n, T310s, T610, T710, and T710s devices.	https://support.ruckuswireless.com/security_bulletins/304	H-RUC-R750-190820/1715

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2020-13914		
Insufficiently Protected Credentials	28-Jul-20	6.4	Insecure permissions in emfd/libemf in Ruckus Wireless Unleashed through 200.7.10.102.92 allow a remote attacker to overwrite admin credentials via an unauthenticated crafted HTTP request. This affects C110, E510, H320, H510, M510, R320, R310, R500, R510 R600, R610, R710, R720, R750, T300, T301n, T301s, T310c, T310d, T310n, T310s, T610, T710, and T710s devices. **CVE ID : CVE-2020-13915**	https://support.ruckuswireless.com/security_bulletins/304	H-RUC-R750-190820/1716
Out-of-bounds Write	28-Jul-20	7.5	A stack buffer overflow in webs in Ruckus Wireless Unleashed through 200.7.10.102.92 allows a remote attacker to execute code via an unauthenticated crafted HTTP request. This affects C110, E510, H320, H510, M510, R320, R310, R500, R510 R600, R610, R710, R720, R750, T300, T301n, T301s, T310c, T310d, T310n, T310s, T610, T710, and T710s devices. **CVE ID : CVE-2020-13916**	https://support.ruckuswireless.com/security_bulletins/304	H-RUC-R750-190820/1717
Improper Neutralization of Special Elements used in an OS Command	28-Jul-20	7.5	rkscli in Ruckus Wireless Unleashed through 200.7.10.92 allows a remote attacker to achieve command injection and jailbreak the CLI via a	https://support.ruckuswireless.com/security_bulletins/304	H-RUC-R750-190820/1718

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
('OS Command Injection')			crafted CLI command. This affects C110, E510, H320, H510, M510, R320, R310, R500, R510 R600, R610, R710, R720, R750, T300, T301n, T301s, T310c, T310d, T310n, T310s, T610, T710, and T710s devices. **CVE ID : CVE-2020-13917**		
Information Exposure	28-Jul-20	5	Incorrect access control in webs in Ruckus Wireless Unleashed through 200.7.10.102.92 allows a remote attacker to leak system information (that can be used for a jailbreak) via an unauthenticated crafted HTTP request. This affects C110, E510, H320, H510, M510, R320, R310, R500, R510 R600, R610, R710, R720, R750, T300, T301n, T301s, T310c, T310d, T310n, T310s, T610, T710, and T710s devices. **CVE ID : CVE-2020-13918**	https://support.ruckuswireless.com/security_bulletins/304	H-RUC-R750-190820/1719
Improper Neutralization of Special Elements used in an OS Command ('OS Command Injection')	28-Jul-20	7.5	emfd/libemf in Ruckus Wireless Unleashed through 200.7.10.102.92 allows a remote attacker to achieve command injection via a crafted HTTP request. This affects C110, E510, H320, H510, M510, R320, R310, R500, R510 R600, R610, R710, R720, R750, T300, T301n, T301s, T310c, T310d,	https://support.ruckuswireless.com/security_bulletins/304	H-RUC-R750-190820/1720

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			T310n, T310s, T610, T710, and T710s devices. **CVE ID : CVE-2020-13919**		
t300					
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	28-Jul-20	4.3	An XSS issue in emfd in Ruckus Wireless Unleashed through 200.7.10.102.92 allows a remote attacker to execute JavaScript code via an unauthenticated crafted HTTP request. This affects C110, E510, H320, H510, M510, R320, R310, R500, R510 R600, R610, R710, R720, R750, T300, T301n, T301s, T310c, T310d, T310n, T310s, T610, T710, and T710s devices. **CVE ID : CVE-2020-13913**	https://support.ruckuswireless.com/security_bulletins/304	H-RUC-T300-190820/1721
Improper Input Validation	28-Jul-20	5	webs in Ruckus Wireless Unleashed through 200.7.10.102.92 allows a remote attacker to cause a denial of service (Segmentation fault) to the webserver via an unauthenticated crafted HTTP request. This affects C110, E510, H320, H510, M510, R320, R310, R500, R510 R600, R610, R710, R720, R750, T300, T301n, T301s, T310c, T310d, T310n, T310s, T610, T710, and T710s devices. **CVE ID : CVE-2020-13914**	https://support.ruckuswireless.com/security_bulletins/304	H-RUC-T300-190820/1722
Insufficiently Protected	28-Jul-20	6.4	Insecure permissions in emfd/libemf in Ruckus	https://support.ruckuswi	H-RUC-T300-190820/1723

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Credentials			Wireless Unleashed through 200.7.10.102.92 allow a remote attacker to overwrite admin credentials via an unauthenticated crafted HTTP request. This affects C110, E510, H320, H510, M510, R320, R310, R500, R510 R600, R610, R710, R720, R750, T300, T301n, T301s, T310c, T310d, T310n, T310s, T610, T710, and T710s devices. **CVE ID : CVE-2020-13915**	reless.com/security_bulletins/304	
Out-of-bounds Write	28-Jul-20	7.5	A stack buffer overflow in webs in Ruckus Wireless Unleashed through 200.7.10.102.92 allows a remote attacker to execute code via an unauthenticated crafted HTTP request. This affects C110, E510, H320, H510, M510, R320, R310, R500, R510 R600, R610, R710, R720, R750, T300, T301n, T301s, T310c, T310d, T310n, T310s, T610, T710, and T710s devices. **CVE ID : CVE-2020-13916**	https://support.ruckuswireless.com/security_bulletins/304	H-RUC-T300-190820/1724
Improper Neutralization of Special Elements used in an OS Command ('OS Command Injection')	28-Jul-20	7.5	rkscli in Ruckus Wireless Unleashed through 200.7.10.92 allows a remote attacker to achieve command injection and jailbreak the CLI via a crafted CLI command. This affects C110, E510, H320, H510, M510, R320, R310,	https://support.ruckuswireless.com/security_bulletins/304	H-RUC-T300-190820/1725

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			R500, R510 R600, R610, R710, R720, R750, T300, T301n, T301s, T310c, T310d, T310n, T310s, T610, T710, and T710s devices. **CVE ID : CVE-2020-13917**		
Information Exposure	28-Jul-20	5	Incorrect access control in webs in Ruckus Wireless Unleashed through 200.7.10.102.92 allows a remote attacker to leak system information (that can be used for a jailbreak) via an unauthenticated crafted HTTP request. This affects C110, E510, H320, H510, M510, R320, R310, R500, R510 R600, R610, R710, R720, R750, T300, T301n, T301s, T310c, T310d, T310n, T310s, T610, T710, and T710s devices. **CVE ID : CVE-2020-13918**	https://support.ruckuswireless.com/security_bulletins/304	H-RUC-T300-190820/1726
Improper Neutralization of Special Elements used in an OS Command ('OS Command Injection')	28-Jul-20	7.5	emfd/libemf in Ruckus Wireless Unleashed through 200.7.10.102.92 allows a remote attacker to achieve command injection via a crafted HTTP request. This affects C110, E510, H320, H510, M510, R320, R310, R500, R510 R600, R610, R710, R720, R750, T300, T301n, T301s, T310c, T310d, T310n, T310s, T610, T710, and T710s devices.	https://support.ruckuswireless.com/security_bulletins/304	H-RUC-T300-190820/1727

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2020-13919		
t301n					
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	28-Jul-20	4.3	An XSS issue in emfd in Ruckus Wireless Unleashed through 200.7.10.102.92 allows a remote attacker to execute JavaScript code via an unauthenticated crafted HTTP request. This affects C110, E510, H320, H510, M510, R320, R310, R500, R510 R600, R610, R710, R720, R750, T300, T301n, T301s, T310c, T310d, T310n, T310s, T610, T710, and T710s devices. **CVE ID : CVE-2020-13913**	https://support.ruckuswireless.com/security_bulletins/304	H-RUC-T301-190820/1728
Improper Input Validation	28-Jul-20	5	webs in Ruckus Wireless Unleashed through 200.7.10.102.92 allows a remote attacker to cause a denial of service (Segmentation fault) to the webserver via an unauthenticated crafted HTTP request. This affects C110, E510, H320, H510, M510, R320, R310, R500, R510 R600, R610, R710, R720, R750, T300, T301n, T301s, T310c, T310d, T310n, T310s, T610, T710, and T710s devices. **CVE ID : CVE-2020-13914**	https://support.ruckuswireless.com/security_bulletins/304	H-RUC-T301-190820/1729
Insufficiently Protected Credentials	28-Jul-20	6.4	Insecure permissions in emfd/libemf in Ruckus Wireless Unleashed through 200.7.10.102.92	https://support.ruckuswireless.com/security_bulle	H-RUC-T301-190820/1730

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			allow a remote attacker to overwrite admin credentials via an unauthenticated crafted HTTP request. This affects C110, E510, H320, H510, M510, R320, R310, R500, R510 R600, R610, R710, R720, R750, T300, T301n, T301s, T310c, T310d, T310n, T310s, T610, T710, and T710s devices. **CVE ID : CVE-2020-13915**	tins/304	
Out-of-bounds Write	28-Jul-20	7.5	A stack buffer overflow in webs in Ruckus Wireless Unleashed through 200.7.10.102.92 allows a remote attacker to execute code via an unauthenticated crafted HTTP request. This affects C110, E510, H320, H510, M510, R320, R310, R500, R510 R600, R610, R710, R720, R750, T300, T301n, T301s, T310c, T310d, T310n, T310s, T610, T710, and T710s devices. **CVE ID : CVE-2020-13916**	https://support.ruckuswireless.com/security_bulletins/304	H-RUC-T301-190820/1731
Improper Neutralization of Special Elements used in an OS Command ('OS Command Injection')	28-Jul-20	7.5	rkscli in Ruckus Wireless Unleashed through 200.7.10.92 allows a remote attacker to achieve command injection and jailbreak the CLI via a crafted CLI command. This affects C110, E510, H320, H510, M510, R320, R310, R500, R510 R600, R610, R710, R720, R750, T300,	https://support.ruckuswireless.com/security_bulletins/304	H-RUC-T301-190820/1732

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			T301n, T301s, T310c, T310d, T310n, T310s, T610, T710, and T710s devices. **CVE ID : CVE-2020-13917**		
Information Exposure	28-Jul-20	5	Incorrect access control in webs in Ruckus Wireless Unleashed through 200.7.10.102.92 allows a remote attacker to leak system information (that can be used for a jailbreak) via an unauthenticated crafted HTTP request. This affects C110, E510, H320, H510, M510, R320, R310, R500, R510 R600, R610, R710, R720, R750, T300, T301n, T301s, T310c, T310d, T310n, T310s, T610, T710, and T710s devices. **CVE ID : CVE-2020-13918**	https://support.ruckuswireless.com/security_bulletins/304	H-RUC-T301-190820/1733
Improper Neutralization of Special Elements used in an OS Command ('OS Command Injection')	28-Jul-20	7.5	emfd/libemf in Ruckus Wireless Unleashed through 200.7.10.102.92 allows a remote attacker to achieve command injection via a crafted HTTP request. This affects C110, E510, H320, H510, M510, R320, R310, R500, R510 R600, R610, R710, R720, R750, T300, T301n, T301s, T310c, T310d, T310n, T310s, T610, T710, and T710s devices. **CVE ID : CVE-2020-13919**	https://support.ruckuswireless.com/security_bulletins/304	H-RUC-T301-190820/1734
t301s					

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	28-Jul-20	4.3	An XSS issue in emfd in Ruckus Wireless Unleashed through 200.7.10.102.92 allows a remote attacker to execute JavaScript code via an unauthenticated crafted HTTP request. This affects C110, E510, H320, H510, M510, R320, R310, R500, R510 R600, R610, R710, R720, R750, T300, T301n, T301s, T310c, T310d, T310n, T310s, T610, T710, and T710s devices. **CVE ID : CVE-2020-13913**	https://support.ruckuswireless.com/security_bulletins/304	H-RUC-T301-190820/1735
Improper Input Validation	28-Jul-20	5	webs in Ruckus Wireless Unleashed through 200.7.10.102.92 allows a remote attacker to cause a denial of service (Segmentation fault) to the webserver via an unauthenticated crafted HTTP request. This affects C110, E510, H320, H510, M510, R320, R310, R500, R510 R600, R610, R710, R720, R750, T300, T301n, T301s, T310c, T310d, T310n, T310s, T610, T710, and T710s devices. **CVE ID : CVE-2020-13914**	https://support.ruckuswireless.com/security_bulletins/304	H-RUC-T301-190820/1736
Insufficiently Protected Credentials	28-Jul-20	6.4	Insecure permissions in emfd/libemf in Ruckus Wireless Unleashed through 200.7.10.102.92 allow a remote attacker to overwrite admin credentials via an	https://support.ruckuswireless.com/security_bulletins/304	H-RUC-T301-190820/1737

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			unauthenticated crafted HTTP request. This affects C110, E510, H320, H510, M510, R320, R310, R500, R510 R600, R610, R710, R720, R750, T300, T301n, T301s, T310c, T310d, T310n, T310s, T610, T710, and T710s devices. **CVE ID : CVE-2020-13915**		
Out-of-bounds Write	28-Jul-20	7.5	A stack buffer overflow in webs in Ruckus Wireless Unleashed through 200.7.10.102.92 allows a remote attacker to execute code via an unauthenticated crafted HTTP request. This affects C110, E510, H320, H510, M510, R320, R310, R500, R510 R600, R610, R710, R720, R750, T300, T301n, T301s, T310c, T310d, T310n, T310s, T610, T710, and T710s devices. **CVE ID : CVE-2020-13916**	https://support.ruckuswireless.com/security_bulletins/304	H-RUC-T301-190820/1738
Improper Neutralization of Special Elements used in an OS Command ('OS Command Injection')	28-Jul-20	7.5	rkscli in Ruckus Wireless Unleashed through 200.7.10.92 allows a remote attacker to achieve command injection and jailbreak the CLI via a crafted CLI command. This affects C110, E510, H320, H510, M510, R320, R310, R500, R510 R600, R610, R710, R720, R750, T300, T301n, T301s, T310c, T310d, T310n, T310s, T610, T710, and T710s	https://support.ruckuswireless.com/security_bulletins/304	H-RUC-T301-190820/1739

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			devices. **CVE ID : CVE-2020-13917**		
Information Exposure	28-Jul-20	5	Incorrect access control in webs in Ruckus Wireless Unleashed through 200.7.10.102.92 allows a remote attacker to leak system information (that can be used for a jailbreak) via an unauthenticated crafted HTTP request. This affects C110, E510, H320, H510, M510, R320, R310, R500, R510 R600, R610, R710, R720, R750, T300, T301n, T301s, T310c, T310d, T310n, T310s, T610, T710, and T710s devices. **CVE ID : CVE-2020-13918**	https://support.ruckuswireless.com/security_bulletins/304	H-RUC-T301-190820/1740
Improper Neutralization of Special Elements used in an OS Command ('OS Command Injection')	28-Jul-20	7.5	emfd/libemf in Ruckus Wireless Unleashed through 200.7.10.102.92 allows a remote attacker to achieve command injection via a crafted HTTP request. This affects C110, E510, H320, H510, M510, R320, R310, R500, R510 R600, R610, R710, R720, R750, T300, T301n, T301s, T310c, T310d, T310n, T310s, T610, T710, and T710s devices. **CVE ID : CVE-2020-13919**	https://support.ruckuswireless.com/security_bulletins/304	H-RUC-T301-190820/1741
t310c					
Improper Neutralization of Input	28-Jul-20	4.3	An XSS issue in emfd in Ruckus Wireless Unleashed through	https://support.ruckuswireless.com/s	H-RUC-T310-190820/1742

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
During Web Page Generation ('Cross-site Scripting')			200.7.10.102.92 allows a remote attacker to execute JavaScript code via an unauthenticated crafted HTTP request. This affects C110, E510, H320, H510, M510, R320, R310, R500, R510 R600, R610, R710, R720, R750, T300, T301n, T301s, T310c, T310d, T310n, T310s, T610, T710, and T710s devices. **CVE ID : CVE-2020-13913**	ecurity_bulletins/304	
Improper Input Validation	28-Jul-20	5	webs in Ruckus Wireless Unleashed through 200.7.10.102.92 allows a remote attacker to cause a denial of service (Segmentation fault) to the webserver via an unauthenticated crafted HTTP request. This affects C110, E510, H320, H510, M510, R320, R310, R500, R510 R600, R610, R710, R720, R750, T300, T301n, T301s, T310c, T310d, T310n, T310s, T610, T710, and T710s devices. **CVE ID : CVE-2020-13914**	https://support.ruckuswireless.com/security_bulletins/304	H-RUC-T310-190820/1743
Insufficiently Protected Credentials	28-Jul-20	6.4	Insecure permissions in emfd/libemf in Ruckus Wireless Unleashed through 200.7.10.102.92 allow a remote attacker to overwrite admin credentials via an unauthenticated crafted HTTP request. This affects C110, E510, H320, H510,	https://support.ruckuswireless.com/security_bulletins/304	H-RUC-T310-190820/1744

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			M510, R320, R310, R500, R510 R600, R610, R710, R720, R750, T300, T301n, T301s, T310c, T310d, T310n, T310s, T610, T710, and T710s devices. **CVE ID : CVE-2020-13915**		
Out-of-bounds Write	28-Jul-20	7.5	A stack buffer overflow in webs in Ruckus Wireless Unleashed through 200.7.10.102.92 allows a remote attacker to execute code via an unauthenticated crafted HTTP request. This affects C110, E510, H320, H510, M510, R320, R310, R500, R510 R600, R610, R710, R720, R750, T300, T301n, T301s, T310c, T310d, T310n, T310s, T610, T710, and T710s devices. **CVE ID : CVE-2020-13916**	https://support.ruckuswireless.com/security_bulletins/304	H-RUC-T310-190820/1745
Improper Neutralization of Special Elements used in an OS Command ('OS Command Injection')	28-Jul-20	7.5	rkscli in Ruckus Wireless Unleashed through 200.7.10.92 allows a remote attacker to achieve command injection and jailbreak the CLI via a crafted CLI command. This affects C110, E510, H320, H510, M510, R320, R310, R500, R510 R600, R610, R710, R720, R750, T300, T301n, T301s, T310c, T310d, T310n, T310s, T610, T710, and T710s devices. **CVE ID : CVE-2020-13917**	https://support.ruckuswireless.com/security_bulletins/304	H-RUC-T310-190820/1746

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Information Exposure	28-Jul-20	5	Incorrect access control in webs in Ruckus Wireless Unleashed through 200.7.10.102.92 allows a remote attacker to leak system information (that can be used for a jailbreak) via an unauthenticated crafted HTTP request. This affects C110, E510, H320, H510, M510, R320, R310, R500, R510 R600, R610, R710, R720, R750, T300, T301n, T301s, T310c, T310d, T310n, T310s, T610, T710, and T710s devices. **CVE ID : CVE-2020-13918**	https://support.ruckuswireless.com/security_bulletins/304	H-RUC-T310-190820/1747
Improper Neutralization of Special Elements used in an OS Command ('OS Command Injection')	28-Jul-20	7.5	emfd/libemf in Ruckus Wireless Unleashed through 200.7.10.102.92 allows a remote attacker to achieve command injection via a crafted HTTP request. This affects C110, E510, H320, H510, M510, R320, R310, R500, R510 R600, R610, R710, R720, R750, T300, T301n, T301s, T310c, T310d, T310n, T310s, T610, T710, and T710s devices. **CVE ID : CVE-2020-13919**	https://support.ruckuswireless.com/security_bulletins/304	H-RUC-T310-190820/1748
t310d					
Improper Neutralization of Input During Web Page Generation	28-Jul-20	4.3	An XSS issue in emfd in Ruckus Wireless Unleashed through 200.7.10.102.92 allows a remote attacker to execute JavaScript code via an	https://support.ruckuswireless.com/security_bulletins/304	H-RUC-T310-190820/1749

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
('Cross-site Scripting')			unauthenticated crafted HTTP request. This affects C110, E510, H320, H510, M510, R320, R310, R500, R510 R600, R610, R710, R720, R750, T300, T301n, T301s, T310c, T310d, T310n, T310s, T610, T710, and T710s devices. **CVE ID : CVE-2020-13913**		
Improper Input Validation	28-Jul-20	5	webs in Ruckus Wireless Unleashed through 200.7.10.102.92 allows a remote attacker to cause a denial of service (Segmentation fault) to the webserver via an unauthenticated crafted HTTP request. This affects C110, E510, H320, H510, M510, R320, R310, R500, R510 R600, R610, R710, R720, R750, T300, T301n, T301s, T310c, T310d, T310n, T310s, T610, T710, and T710s devices. **CVE ID : CVE-2020-13914**	https://support.ruckuswireless.com/security_bulletins/304	H-RUC-T310-190820/1750
Insufficiently Protected Credentials	28-Jul-20	6.4	Insecure permissions in emfd/libemf in Ruckus Wireless Unleashed through 200.7.10.102.92 allow a remote attacker to overwrite admin credentials via an unauthenticated crafted HTTP request. This affects C110, E510, H320, H510, M510, R320, R310, R500, R510 R600, R610, R710, R720, R750, T300, T301n,	https://support.ruckuswireless.com/security_bulletins/304	H-RUC-T310-190820/1751

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			T301s, T310c, T310d, T310n, T310s, T610, T710, and T710s devices. **CVE ID : CVE-2020-13915**		
Out-of-bounds Write	28-Jul-20	7.5	A stack buffer overflow in webs in Ruckus Wireless Unleashed through 200.7.10.102.92 allows a remote attacker to execute code via an unauthenticated crafted HTTP request. This affects C110, E510, H320, H510, M510, R320, R310, R500, R510 R600, R610, R710, R720, R750, T300, T301n, T301s, T310c, T310d, T310n, T310s, T610, T710, and T710s devices. **CVE ID : CVE-2020-13916**	https://support.ruckuswireless.com/security_bulletins/304	H-RUC-T310-190820/1752
Improper Neutralization of Special Elements used in an OS Command ('OS Command Injection')	28-Jul-20	7.5	rkscli in Ruckus Wireless Unleashed through 200.7.10.92 allows a remote attacker to achieve command injection and jailbreak the CLI via a crafted CLI command. This affects C110, E510, H320, H510, M510, R320, R310, R500, R510 R600, R610, R710, R720, R750, T300, T301n, T301s, T310c, T310d, T310n, T310s, T610, T710, and T710s devices. **CVE ID : CVE-2020-13917**	https://support.ruckuswireless.com/security_bulletins/304	H-RUC-T310-190820/1753
Information Exposure	28-Jul-20	5	Incorrect access control in webs in Ruckus Wireless Unleashed through	https://support.ruckuswireless.com/s	H-RUC-T310-190820/1754

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			200.7.10.102.92 allows a remote attacker to leak system information (that can be used for a jailbreak) via an unauthenticated crafted HTTP request. This affects C110, E510, H320, H510, M510, R320, R310, R500, R510 R600, R610, R710, R720, R750, T300, T301n, T301s, T310c, T310d, T310n, T310s, T610, T710, and T710s devices. **CVE ID : CVE-2020-13918**	ecurity_bulletins/304	
Improper Neutralization of Special Elements used in an OS Command ('OS Command Injection')	28-Jul-20	7.5	emfd/libemf in Ruckus Wireless Unleashed through 200.7.10.102.92 allows a remote attacker to achieve command injection via a crafted HTTP request. This affects C110, E510, H320, H510, M510, R320, R310, R500, R510 R600, R610, R710, R720, R750, T300, T301n, T301s, T310c, T310d, T310n, T310s, T610, T710, and T710s devices. **CVE ID : CVE-2020-13919**	https://support.ruckuswireless.com/security_bulletins/304	H-RUC-T310-190820/1755
t310n					
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	28-Jul-20	4.3	An XSS issue in emfd in Ruckus Wireless Unleashed through 200.7.10.102.92 allows a remote attacker to execute JavaScript code via an unauthenticated crafted HTTP request. This affects C110, E510, H320, H510,	https://support.ruckuswireless.com/security_bulletins/304	H-RUC-T310-190820/1756

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			M510, R320, R310, R500, R510 R600, R610, R710, R720, R750, T300, T301n, T301s, T310c, T310d, T310n, T310s, T610, T710, and T710s devices. **CVE ID : CVE-2020-13913**		
Improper Input Validation	28-Jul-20	5	webs in Ruckus Wireless Unleashed through 200.7.10.102.92 allows a remote attacker to cause a denial of service (Segmentation fault) to the webserver via an unauthenticated crafted HTTP request. This affects C110, E510, H320, H510, M510, R320, R310, R500, R510 R600, R610, R710, R720, R750, T300, T301n, T301s, T310c, T310d, T310n, T310s, T610, T710, and T710s devices. **CVE ID : CVE-2020-13914**	https://support.ruckuswireless.com/security_bulletins/304	H-RUC-T310-190820/1757
Insufficiently Protected Credentials	28-Jul-20	6.4	Insecure permissions in emfd/libemf in Ruckus Wireless Unleashed through 200.7.10.102.92 allow a remote attacker to overwrite admin credentials via an unauthenticated crafted HTTP request. This affects C110, E510, H320, H510, M510, R320, R310, R500, R510 R600, R610, R710, R720, R750, T300, T301n, T301s, T310c, T310d, T310n, T310s, T610, T710, and T710s devices.	https://support.ruckuswireless.com/security_bulletins/304	H-RUC-T310-190820/1758

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2020-13915		
Out-of-bounds Write	28-Jul-20	7.5	A stack buffer overflow in webs in Ruckus Wireless Unleashed through 200.7.10.102.92 allows a remote attacker to execute code via an unauthenticated crafted HTTP request. This affects C110, E510, H320, H510, M510, R320, R310, R500, R510 R600, R610, R710, R720, R750, T300, T301n, T301s, T310c, T310d, T310n, T310s, T610, T710, and T710s devices. **CVE ID : CVE-2020-13916**	https://support.ruckuswireless.com/security_bulletins/304	H-RUC-T310-190820/1759
Improper Neutralization of Special Elements used in an OS Command ('OS Command Injection')	28-Jul-20	7.5	rkscli in Ruckus Wireless Unleashed through 200.7.10.92 allows a remote attacker to achieve command injection and jailbreak the CLI via a crafted CLI command. This affects C110, E510, H320, H510, M510, R320, R310, R500, R510 R600, R610, R710, R720, R750, T300, T301n, T301s, T310c, T310d, T310n, T310s, T610, T710, and T710s devices. **CVE ID : CVE-2020-13917**	https://support.ruckuswireless.com/security_bulletins/304	H-RUC-T310-190820/1760
Information Exposure	28-Jul-20	5	Incorrect access control in webs in Ruckus Wireless Unleashed through 200.7.10.102.92 allows a remote attacker to leak system information (that can be used for a jailbreak)	https://support.ruckuswireless.com/security_bulletins/304	H-RUC-T310-190820/1761

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			via an unauthenticated crafted HTTP request. This affects C110, E510, H320, H510, M510, R320, R310, R500, R510 R600, R610, R710, R720, R750, T300, T301n, T301s, T310c, T310d, T310n, T310s, T610, T710, and T710s devices. **CVE ID : CVE-2020-13918**		
Improper Neutralization of Special Elements used in an OS Command ('OS Command Injection')	28-Jul-20	7.5	emfd/libemf in Ruckus Wireless Unleashed through 200.7.10.102.92 allows a remote attacker to achieve command injection via a crafted HTTP request. This affects C110, E510, H320, H510, M510, R320, R310, R500, R510 R600, R610, R710, R720, R750, T300, T301n, T301s, T310c, T310d, T310n, T310s, T610, T710, and T710s devices. **CVE ID : CVE-2020-13919**	https://support.ruckuswireless.com/security_bulletins/304	H-RUC-T310-190820/1762
t310s					
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	28-Jul-20	4.3	An XSS issue in emfd in Ruckus Wireless Unleashed through 200.7.10.102.92 allows a remote attacker to execute JavaScript code via an unauthenticated crafted HTTP request. This affects C110, E510, H320, H510, M510, R320, R310, R500, R510 R600, R610, R710, R720, R750, T300, T301n, T301s, T310c, T310d,	https://support.ruckuswireless.com/security_bulletins/304	H-RUC-T310-190820/1763

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			T310n, T310s, T610, T710, and T710s devices. **CVE ID : CVE-2020-13913**		
Improper Input Validation	28-Jul-20	5	webs in Ruckus Wireless Unleashed through 200.7.10.102.92 allows a remote attacker to cause a denial of service (Segmentation fault) to the webserver via an unauthenticated crafted HTTP request. This affects C110, E510, H320, H510, M510, R320, R310, R500, R510 R600, R610, R710, R720, R750, T300, T301n, T301s, T310c, T310d, T310n, T310s, T610, T710, and T710s devices. **CVE ID : CVE-2020-13914**	https://support.ruckuswireless.com/security_bulletins/304	H-RUC-T310-190820/1764
Insufficiently Protected Credentials	28-Jul-20	6.4	Insecure permissions in emfd/libemf in Ruckus Wireless Unleashed through 200.7.10.102.92 allow a remote attacker to overwrite admin credentials via an unauthenticated crafted HTTP request. This affects C110, E510, H320, H510, M510, R320, R310, R500, R510 R600, R610, R710, R720, R750, T300, T301n, T301s, T310c, T310d, T310n, T310s, T610, T710, and T710s devices. **CVE ID : CVE-2020-13915**	https://support.ruckuswireless.com/security_bulletins/304	H-RUC-T310-190820/1765
Out-of-bounds	28-Jul-20	7.5	A stack buffer overflow in webs in Ruckus Wireless	https://support.ruckuswi	H-RUC-T310-190820/1766

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Write			Unleashed through 200.7.10.102.92 allows a remote attacker to execute code via an unauthenticated crafted HTTP request. This affects C110, E510, H320, H510, M510, R320, R310, R500, R510 R600, R610, R710, R720, R750, T300, T301n, T301s, T310c, T310d, T310n, T310s, T610, T710, and T710s devices. **CVE ID : CVE-2020-13916**	reless.com/security_bulletins/304	
Improper Neutralization of Special Elements used in an OS Command ('OS Command Injection')	28-Jul-20	7.5	rkscli in Ruckus Wireless Unleashed through 200.7.10.92 allows a remote attacker to achieve command injection and jailbreak the CLI via a crafted CLI command. This affects C110, E510, H320, H510, M510, R320, R310, R500, R510 R600, R610, R710, R720, R750, T300, T301n, T301s, T310c, T310d, T310n, T310s, T610, T710, and T710s devices. **CVE ID : CVE-2020-13917**	https://support.ruckuswireless.com/security_bulletins/304	H-RUC-T310-190820/1767
Information Exposure	28-Jul-20	5	Incorrect access control in webs in Ruckus Wireless Unleashed through 200.7.10.102.92 allows a remote attacker to leak system information (that can be used for a jailbreak) via an unauthenticated crafted HTTP request. This affects C110, E510, H320,	https://support.ruckuswireless.com/security_bulletins/304	H-RUC-T310-190820/1768

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			H510, M510, R320, R310, R500, R510 R600, R610, R710, R720, R750, T300, T301n, T301s, T310c, T310d, T310n, T310s, T610, T710, and T710s devices. **CVE ID : CVE-2020-13918**		
Improper Neutralization of Special Elements used in an OS Command ('OS Command Injection')	28-Jul-20	7.5	emfd/libemf in Ruckus Wireless Unleashed through 200.7.10.102.92 allows a remote attacker to achieve command injection via a crafted HTTP request. This affects C110, E510, H320, H510, M510, R320, R310, R500, R510 R600, R610, R710, R720, R750, T300, T301n, T301s, T310c, T310d, T310n, T310s, T610, T710, and T710s devices. **CVE ID : CVE-2020-13919**	https://support.ruckuswireless.com/security_bulletins/304	H-RUC-T310-190820/1769
t610					
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	28-Jul-20	4.3	An XSS issue in emfd in Ruckus Wireless Unleashed through 200.7.10.102.92 allows a remote attacker to execute JavaScript code via an unauthenticated crafted HTTP request. This affects C110, E510, H320, H510, M510, R320, R310, R500, R510 R600, R610, R710, R720, R750, T300, T301n, T301s, T310c, T310d, T310n, T310s, T610, T710, and T710s devices.	https://support.ruckuswireless.com/security_bulletins/304	H-RUC-T610-190820/1770

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2020-13913		
Improper Input Validation	28-Jul-20	5	webs in Ruckus Wireless Unleashed through 200.7.10.102.92 allows a remote attacker to cause a denial of service (Segmentation fault) to the webserver via an unauthenticated crafted HTTP request. This affects C110, E510, H320, H510, M510, R320, R310, R500, R510 R600, R610, R710, R720, R750, T300, T301n, T301s, T310c, T310d, T310n, T310s, T610, T710, and T710s devices. **CVE ID : CVE-2020-13914**	https://support.ruckuswireless.com/security_bulletins/304	H-RUC-T610-190820/1771
Insufficiently Protected Credentials	28-Jul-20	6.4	Insecure permissions in emfd/libemf in Ruckus Wireless Unleashed through 200.7.10.102.92 allow a remote attacker to overwrite admin credentials via an unauthenticated crafted HTTP request. This affects C110, E510, H320, H510, M510, R320, R310, R500, R510 R600, R610, R710, R720, R750, T300, T301n, T301s, T310c, T310d, T310n, T310s, T610, T710, and T710s devices. **CVE ID : CVE-2020-13915**	https://support.ruckuswireless.com/security_bulletins/304	H-RUC-T610-190820/1772
Out-of-bounds Write	28-Jul-20	7.5	A stack buffer overflow in webs in Ruckus Wireless Unleashed through 200.7.10.102.92 allows a remote attacker to execute	https://support.ruckuswireless.com/security_bulle	H-RUC-T610-190820/1773

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			code via an unauthenticated crafted HTTP request. This affects C110, E510, H320, H510, M510, R320, R310, R500, R510 R600, R610, R710, R720, R750, T300, T301n, T301s, T310c, T310d, T310n, T310s, T610, T710, and T710s devices. **CVE ID : CVE-2020-13916**	tins/304	
Improper Neutralization of Special Elements used in an OS Command ('OS Command Injection')	28-Jul-20	7.5	rkscli in Ruckus Wireless Unleashed through 200.7.10.92 allows a remote attacker to achieve command injection and jailbreak the CLI via a crafted CLI command. This affects C110, E510, H320, H510, M510, R320, R310, R500, R510 R600, R610, R710, R720, R750, T300, T301n, T301s, T310c, T310d, T310n, T310s, T610, T710, and T710s devices. **CVE ID : CVE-2020-13917**	https://support.ruckuswireless.com/security_bulletins/304	H-RUC-T610-190820/1774
Information Exposure	28-Jul-20	5	Incorrect access control in webs in Ruckus Wireless Unleashed through 200.7.10.102.92 allows a remote attacker to leak system information (that can be used for a jailbreak) via an unauthenticated crafted HTTP request. This affects C110, E510, H320, H510, M510, R320, R310, R500, R510 R600, R610, R710, R720, R750, T300,	https://support.ruckuswireless.com/security_bulletins/304	H-RUC-T610-190820/1775

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			T301n, T301s, T310c, T310d, T310n, T310s, T610, T710, and T710s devices. **CVE ID : CVE-2020-13918**		
Improper Neutralization of Special Elements used in an OS Command ('OS Command Injection')	28-Jul-20	7.5	emfd/libemf in Ruckus Wireless Unleashed through 200.7.10.102.92 allows a remote attacker to achieve command injection via a crafted HTTP request. This affects C110, E510, H320, H510, M510, R320, R310, R500, R510 R600, R610, R710, R720, R750, T300, T301n, T301s, T310c, T310d, T310n, T310s, T610, T710, and T710s devices. **CVE ID : CVE-2020-13919**	https://support.ruckuswireless.com/security_bulletins/304	H-RUC-T610-190820/1776
t710					
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	28-Jul-20	4.3	An XSS issue in emfd in Ruckus Wireless Unleashed through 200.7.10.102.92 allows a remote attacker to execute JavaScript code via an unauthenticated crafted HTTP request. This affects C110, E510, H320, H510, M510, R320, R310, R500, R510 R600, R610, R710, R720, R750, T300, T301n, T301s, T310c, T310d, T310n, T310s, T610, T710, and T710s devices. **CVE ID : CVE-2020-13913**	https://support.ruckuswireless.com/security_bulletins/304	H-RUC-T710-190820/1777
Improper Input	28-Jul-20	5	webs in Ruckus Wireless Unleashed through	https://support.ruckuswi	H-RUC-T710-190820/1778

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Validation			200.7.10.102.92 allows a remote attacker to cause a denial of service (Segmentation fault) to the webserver via an unauthenticated crafted HTTP request. This affects C110, E510, H320, H510, M510, R320, R310, R500, R510 R600, R610, R710, R720, R750, T300, T301n, T301s, T310c, T310d, T310n, T310s, T610, T710, and T710s devices. **CVE ID : CVE-2020-13914**	reless.com/security_bulletins/304	
Insufficiently Protected Credentials	28-Jul-20	6.4	Insecure permissions in emfd/libemf in Ruckus Wireless Unleashed through 200.7.10.102.92 allow a remote attacker to overwrite admin credentials via an unauthenticated crafted HTTP request. This affects C110, E510, H320, H510, M510, R320, R310, R500, R510 R600, R610, R710, R720, R750, T300, T301n, T301s, T310c, T310d, T310n, T310s, T610, T710, and T710s devices. **CVE ID : CVE-2020-13915**	https://support.ruckuswireless.com/security_bulletins/304	H-RUC-T710-190820/1779
Out-of-bounds Write	28-Jul-20	7.5	A stack buffer overflow in webs in Ruckus Wireless Unleashed through 200.7.10.102.92 allows a remote attacker to execute code via an unauthenticated crafted HTTP request. This affects	https://support.ruckuswireless.com/security_bulletins/304	H-RUC-T710-190820/1780

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			C110, E510, H320, H510, M510, R320, R310, R500, R510 R600, R610, R710, R720, R750, T300, T301n, T301s, T310c, T310d, T310n, T310s, T610, T710, and T710s devices. **CVE ID : CVE-2020-13916**		
Improper Neutralization of Special Elements used in an OS Command ('OS Command Injection')	28-Jul-20	7.5	rkscli in Ruckus Wireless Unleashed through 200.7.10.92 allows a remote attacker to achieve command injection and jailbreak the CLI via a crafted CLI command. This affects C110, E510, H320, H510, M510, R320, R310, R500, R510 R600, R610, R710, R720, R750, T300, T301n, T301s, T310c, T310d, T310n, T310s, T610, T710, and T710s devices. **CVE ID : CVE-2020-13917**	https://support.ruckuswireless.com/security_bulletins/304	H-RUC-T710-190820/1781
Information Exposure	28-Jul-20	5	Incorrect access control in webs in Ruckus Wireless Unleashed through 200.7.10.102.92 allows a remote attacker to leak system information (that can be used for a jailbreak) via an unauthenticated crafted HTTP request. This affects C110, E510, H320, H510, M510, R320, R310, R500, R510 R600, R610, R710, R720, R750, T300, T301n, T301s, T310c, T310d, T310n, T310s, T610, T710, and T710s	https://support.ruckuswireless.com/security_bulletins/304	H-RUC-T710-190820/1782

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			devices. **CVE ID : CVE-2020-13918**		
Improper Neutralization of Special Elements used in an OS Command ('OS Command Injection')	28-Jul-20	7.5	emfd/libemf in Ruckus Wireless Unleashed through 200.7.10.102.92 allows a remote attacker to achieve command injection via a crafted HTTP request. This affects C110, E510, H320, H510, M510, R320, R310, R500, R510 R600, R610, R710, R720, R750, T300, T301n, T301s, T310c, T310d, T310n, T310s, T610, T710, and T710s devices. **CVE ID : CVE-2020-13919**	https://support.ruckuswireless.com/security_bulletins/304	H-RUC-T710-190820/1783
t710s					
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	28-Jul-20	4.3	An XSS issue in emfd in Ruckus Wireless Unleashed through 200.7.10.102.92 allows a remote attacker to execute JavaScript code via an unauthenticated crafted HTTP request. This affects C110, E510, H320, H510, M510, R320, R310, R500, R510 R600, R610, R710, R720, R750, T300, T301n, T301s, T310c, T310d, T310n, T310s, T610, T710, and T710s devices. **CVE ID : CVE-2020-13913**	https://support.ruckuswireless.com/security_bulletins/304	H-RUC-T710-190820/1784
Improper Input Validation	28-Jul-20	5	webs in Ruckus Wireless Unleashed through 200.7.10.102.92 allows a remote attacker to cause a denial of service	https://support.ruckuswireless.com/security_bulletins/304	H-RUC-T710-190820/1785

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			(Segmentation fault) to the webserver via an unauthenticated crafted HTTP request. This affects C110, E510, H320, H510, M510, R320, R310, R500, R510 R600, R610, R710, R720, R750, T300, T301n, T301s, T310c, T310d, T310n, T310s, T610, T710, and T710s devices. **CVE ID : CVE-2020-13914**		
Insufficiently Protected Credentials	28-Jul-20	6.4	Insecure permissions in emfd/libemf in Ruckus Wireless Unleashed through 200.7.10.102.92 allow a remote attacker to overwrite admin credentials via an unauthenticated crafted HTTP request. This affects C110, E510, H320, H510, M510, R320, R310, R500, R510 R600, R610, R710, R720, R750, T300, T301n, T301s, T310c, T310d, T310n, T310s, T610, T710, and T710s devices. **CVE ID : CVE-2020-13915**	https://support.ruckuswireless.com/security_bulletins/304	H-RUC-T710-190820/1786
Out-of-bounds Write	28-Jul-20	7.5	A stack buffer overflow in webs in Ruckus Wireless Unleashed through 200.7.10.102.92 allows a remote attacker to execute code via an unauthenticated crafted HTTP request. This affects C110, E510, H320, H510, M510, R320, R310, R500, R510 R600, R610, R710,	https://support.ruckuswireless.com/security_bulletins/304	H-RUC-T710-190820/1787

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			R720, R750, T300, T301n, T301s, T310c, T310d, T310n, T310s, T610, T710, and T710s devices. **CVE ID : CVE-2020-13916**		
Improper Neutralization of Special Elements used in an OS Command ('OS Command Injection')	28-Jul-20	7.5	rkscli in Ruckus Wireless Unleashed through 200.7.10.92 allows a remote attacker to achieve command injection and jailbreak the CLI via a crafted CLI command. This affects C110, E510, H320, H510, M510, R320, R310, R500, R510 R600, R610, R710, R720, R750, T300, T301n, T301s, T310c, T310d, T310n, T310s, T610, T710, and T710s devices. **CVE ID : CVE-2020-13917**	https://support.ruckuswireless.com/security_bulletins/304	H-RUC-T710-190820/1788
Information Exposure	28-Jul-20	5	Incorrect access control in webs in Ruckus Wireless Unleashed through 200.7.10.102.92 allows a remote attacker to leak system information (that can be used for a jailbreak) via an unauthenticated crafted HTTP request. This affects C110, E510, H320, H510, M510, R320, R310, R500, R510 R600, R610, R710, R720, R750, T300, T301n, T301s, T310c, T310d, T310n, T310s, T610, T710, and T710s devices. **CVE ID : CVE-2020-13918**	https://support.ruckuswireless.com/security_bulletins/304	H-RUC-T710-190820/1789

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Improper Neutralization of Special Elements used in an OS Command ('OS Command Injection')	28-Jul-20	7.5	emfd/libemf in Ruckus Wireless Unleashed through 200.7.10.102.92 allows a remote attacker to achieve command injection via a crafted HTTP request. This affects C110, E510, H320, H510, M510, R320, R310, R500, R510 R600, R610, R710, R720, R750, T300, T301n, T301s, T310c, T310d, T310n, T310s, T610, T710, and T710s devices. **CVE ID : CVE-2020-13919**	https://support.ruckuswireless.com/security_bulletins/304	H-RUC-T710-190820/1790
r310					
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	28-Jul-20	4.3	An XSS issue in emfd in Ruckus Wireless Unleashed through 200.7.10.102.92 allows a remote attacker to execute JavaScript code via an unauthenticated crafted HTTP request. This affects C110, E510, H320, H510, M510, R320, R310, R500, R510 R600, R610, R710, R720, R750, T300, T301n, T301s, T310c, T310d, T310n, T310s, T610, T710, and T710s devices. **CVE ID : CVE-2020-13913**	https://support.ruckuswireless.com/security_bulletins/304	H-RUC-R310-190820/1791
Improper Input Validation	28-Jul-20	5	webs in Ruckus Wireless Unleashed through 200.7.10.102.92 allows a remote attacker to cause a denial of service (Segmentation fault) to the webserver via an unauthenticated crafted	https://support.ruckuswireless.com/security_bulletins/304	H-RUC-R310-190820/1792

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			HTTP request. This affects C110, E510, H320, H510, M510, R320, R310, R500, R510 R600, R610, R710, R720, R750, T300, T301n, T301s, T310c, T310d, T310n, T310s, T610, T710, and T710s devices. **CVE ID : CVE-2020-13914**		
Insufficiently Protected Credentials	28-Jul-20	6.4	Insecure permissions in emfd/libemf in Ruckus Wireless Unleashed through 200.7.10.102.92 allow a remote attacker to overwrite admin credentials via an unauthenticated crafted HTTP request. This affects C110, E510, H320, H510, M510, R320, R310, R500, R510 R600, R610, R710, R720, R750, T300, T301n, T301s, T310c, T310d, T310n, T310s, T610, T710, and T710s devices. **CVE ID : CVE-2020-13915**	https://support.ruckuswireless.com/security_bulletins/304	H-RUC-R310-190820/1793
Out-of-bounds Write	28-Jul-20	7.5	A stack buffer overflow in webs in Ruckus Wireless Unleashed through 200.7.10.102.92 allows a remote attacker to execute code via an unauthenticated crafted HTTP request. This affects C110, E510, H320, H510, M510, R320, R310, R500, R510 R600, R610, R710, R720, R750, T300, T301n, T301s, T310c, T310d, T310n, T310s, T610, T710,	https://support.ruckuswireless.com/security_bulletins/304	H-RUC-R310-190820/1794

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			and T710s devices. **CVE ID : CVE-2020-13916**		
Improper Neutralization of Special Elements used in an OS Command ('OS Command Injection')	28-Jul-20	7.5	rkscli in Ruckus Wireless Unleashed through 200.7.10.92 allows a remote attacker to achieve command injection and jailbreak the CLI via a crafted CLI command. This affects C110, E510, H320, H510, M510, R320, R310, R500, R510 R600, R610, R710, R720, R750, T300, T301n, T301s, T310c, T310d, T310n, T310s, T610, T710, and T710s devices. **CVE ID : CVE-2020-13917**	https://support.ruckuswireless.com/security_bulletins/304	H-RUC-R310-190820/1795
Information Exposure	28-Jul-20	5	Incorrect access control in webs in Ruckus Wireless Unleashed through 200.7.10.102.92 allows a remote attacker to leak system information (that can be used for a jailbreak) via an unauthenticated crafted HTTP request. This affects C110, E510, H320, H510, M510, R320, R310, R500, R510 R600, R610, R710, R720, R750, T300, T301n, T301s, T310c, T310d, T310n, T310s, T610, T710, and T710s devices. **CVE ID : CVE-2020-13918**	https://support.ruckuswireless.com/security_bulletins/304	H-RUC-R310-190820/1796
Improper Neutralization of Special	28-Jul-20	7.5	emfd/libemf in Ruckus Wireless Unleashed through 200.7.10.102.92	https://support.ruckuswireless.com/s	H-RUC-R310-190820/1797

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Elements used in an OS Command ('OS Command Injection')			allows a remote attacker to achieve command injection via a crafted HTTP request. This affects C110, E510, H320, H510, M510, R320, R310, R500, R510 R600, R610, R710, R720, R750, T300, T301n, T301s, T310c, T310d, T310n, T310s, T610, T710, and T710s devices. **CVE ID : CVE-2020-13919**	ecurity_bulletins/304	
Schneider-electric					
tricon_tcm_4351					
Information Exposure	23-Jul-20	5	**VERSION NOT SUPPORTED WHEN ASSIGNED** A legacy debug port account in TCMs installed in Tricon system versions 10.2.0 through 10.5.3 is visible on the network and could allow inappropriate access. This vulnerability was remediated in TCM version 10.5.4. **CVE ID : CVE-2020-7491**	N/A	H-SCH-TRIC-190820/1798
tricon_tcm_4352					
Information Exposure	23-Jul-20	5	**VERSION NOT SUPPORTED WHEN ASSIGNED** A legacy debug port account in TCMs installed in Tricon system versions 10.2.0 through 10.5.3 is visible on the network and could allow inappropriate access. This vulnerability was remediated in TCM	N/A	H-SCH-TRIC-190820/1799

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			version 10.5.4. **CVE ID : CVE-2020-7491**		
tricon_tcm_4351a					
Information Exposure	23-Jul-20	5	**VERSION NOT SUPPORTED WHEN ASSIGNED** A legacy debug port account in TCMs installed in Tricon system versions 10.2.0 through 10.5.3 is visible on the network and could allow inappropriate access. This vulnerability was remediated in TCM version 10.5.4. **CVE ID : CVE-2020-7491**	N/A	H-SCH-TRIC-190820/1800
tricon_tcm_4351b					
Information Exposure	23-Jul-20	5	**VERSION NOT SUPPORTED WHEN ASSIGNED** A legacy debug port account in TCMs installed in Tricon system versions 10.2.0 through 10.5.3 is visible on the network and could allow inappropriate access. This vulnerability was remediated in TCM version 10.5.4. **CVE ID : CVE-2020-7491**	N/A	H-SCH-TRIC-190820/1801
tricon_tcm_4352a					
Information Exposure	23-Jul-20	5	**VERSION NOT SUPPORTED WHEN ASSIGNED** A legacy debug port account in TCMs installed in Tricon system versions 10.2.0 through 10.5.3 is visible on	N/A	H-SCH-TRIC-190820/1802

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			the network and could allow inappropriate access. This vulnerability was remediated in TCM version 10.5.4. **CVE ID : CVE-2020-7491**		
tricon_tcm_4352b					
Information Exposure	23-Jul-20	5	**VERSION NOT SUPPORTED WHEN ASSIGNED** A legacy debug port account in TCMs installed in Tricon system versions 10.2.0 through 10.5.3 is visible on the network and could allow inappropriate access. This vulnerability was remediated in TCM version 10.5.4. **CVE ID : CVE-2020-7491**	N/A	H-SCH-TRIC-190820/1803
teltonika-networks					
gateway_trb245					
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	17-Jul-20	3.5	Insufficient output sanitization in Teltonika firmware TRB2_R_00.02.02 allows a remote, authenticated attacker to conduct persistent cross-site scripting (XSS) attacks by injecting malicious client-side code into the 'URL/ Host / Connection' form in the 'DATA TO SERVER' configuration section. **CVE ID : CVE-2020-5769**	https://www.tenable.com/security/research/tra-2020-43-0	H-TEL-GATE-190820/1804
Tenda					
ac15					

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Improper Neutralization of Special Elements used in an OS Command ('OS Command Injection')	23-Jul-20	10	goform/AdvSetLanip endpoint on Tenda AC15 AC1900 15.03.05.19 devices allows remote attackers to execute arbitrary system commands via shell metacharacters in the lanIp POST parameter. **CVE ID : CVE-2020-15916**	N/A	H-TEN-AC15-190820/1805
Tesla					
model_3					
N/A	23-Jul-20	3.3	** DISPUTED ** Tesla Model 3 vehicles allow attackers to open a door by leveraging access to a legitimate key card, and then using NFC Relay. NOTE: the vendor has developed Pin2Drive to mitigate this issue. **CVE ID : CVE-2020-15912**	N/A	H-TES-MODE-190820/1806
Veeam					
one					
Improper Restriction of XML External Entity Reference ('XXE')	28-Jul-20	7.8	This vulnerability allows remote attackers to disclose sensitive information on affected installations of Veeam ONE 10.0.0.750_20200415. Authentication is not required to exploit this vulnerability. The specific flaw exists within the SSRSReport class. Due to the improper restriction of XML External Entity (XXE) references, a specially crafted document	N/A	H-VEE-ONE-190820/1807

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			specifying a URI causes the XML parser to access the URI and embed the contents back into the XML document for further processing. An attacker can leverage this vulnerability to disclose file contents in the context of SYSTEM. Was ZDI-CAN-10709. **CVE ID : CVE-2020-15418**		
Improper Restriction of XML External Entity Reference ('XXE')	28-Jul-20	7.8	This vulnerability allows remote attackers to disclose sensitive information on affected installations of Veeam ONE 10.0.0.750_20200415. Authentication is not required to exploit this vulnerability. The specific flaw exists within the Reporter_ImportLicense class. Due to the improper restriction of XML External Entity (XXE) references, a specially crafted document specifying a URI causes the XML parser to access the URI and embed the contents back into the XML document for further processing. An attacker can leverage this vulnerability to disclose file contents in the context of SYSTEM. Was ZDI-CAN-10710. **CVE ID : CVE-2020-15419**	N/A	H-VEE-ONE-190820/1808
ZTE					

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
r8500g4					
Improper Authentication	20-Jul-20	7.5	The server management software module of ZTE has an authentication issue vulnerability, which allows users to skip the authentication of the server and execute some commands for high-level users. This affects: <R5300G4V03.08.0100/V03.07.0300/V03.07.0200/V03.07.0108/V03.07.0100/V03.05.0047/V03.05.0046/V03.05.0045/V03.05.0044/V03.05.0043/V03.05.0040/V03.04.0020;R8500G4V03.07.0103/V03.07.0101/V03.06.0100/V03.05.0400/V03.05.0020;R5500G4V03.08.0100/V03.07.0200/V03.07.0100/V03.06.0100> **CVE ID : CVE-2020-6871**	N/A	H-ZTE-R850-190820/1809
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	20-Jul-20	4.3	The server management software module of ZTE has a storage XSS vulnerability. The attacker inserts some attack codes through the foreground login page, which will cause the user to execute the predefined malicious script in the browser. This affects <R5300G4V03.08.0100/V03.07.0300/V03.07.0200/V03.07.0108/V03.07.0100/V03.05.0047/V03.05.0046/V03.05.0045/V03.05.00	N/A	H-ZTE-R850-190820/1810

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			44/V03.05.0043/V03.05.0040/V03.04.0020;R8500G4V03.07.0103/V03.07.0101/V03.06.0100/V03.05.0400/V03.05.0020;R5500G4V03.08.0100/V03.07.0200/V03.07.0100/V03.06.0100>. **CVE ID : CVE-2020-6872**		
r5500g4					
Improper Authentication	20-Jul-20	7.5	The server management software module of ZTE has an authentication issue vulnerability, which allows users to skip the authentication of the server and execute some commands for high-level users. This affects: <R5300G4V03.08.0100/V03.07.0300/V03.07.0200/V03.07.0108/V03.07.0100/V03.05.0047/V03.05.0046/V03.05.0045/V03.05.0044/V03.05.0043/V03.05.0040/V03.04.0020;R8500G4V03.07.0103/V03.07.0101/V03.06.0100/V03.05.0400/V03.05.0020;R5500G4V03.08.0100/V03.07.0200/V03.07.0100/V03.06.0100> **CVE ID : CVE-2020-6871**	N/A	H-ZTE-R550-190820/1811
Improper Neutralization of Input During Web Page Generation ('Cross-site	20-Jul-20	4.3	The server management software module of ZTE has a storage XSS vulnerability. The attacker inserts some attack codes through the foreground login page, which will	N/A	H-ZTE-R550-190820/1812

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Scripting')			cause the user to execute the predefined malicious script in the browser. This affects <R5300G4V03.08.0100/V03.07.0300/V03.07.0200/V03.07.0108/V03.07.0100/V03.05.0047/V03.05.0046/V03.05.0045/V03.05.0044/V03.05.0043/V03.05.0040/V03.04.0020;R8500G4V03.07.0103/V03.07.0101/V03.06.0100/V03.05.0400/V03.05.0020;R5500G4V03.08.0100/V03.07.0200/V03.07.0100/V03.06.0100>. **CVE ID : CVE-2020-6872**		
r5300g4					
Improper Authentication	20-Jul-20	7.5	The server management software module of ZTE has an authentication issue vulnerability, which allows users to skip the authentication of the server and execute some commands for high-level users. This affects: <R5300G4V03.08.0100/V03.07.0300/V03.07.0200/V03.07.0108/V03.07.0100/V03.05.0047/V03.05.0046/V03.05.0045/V03.05.0044/V03.05.0043/V03.05.0040/V03.04.0020;R8500G4V03.07.0103/V03.07.0101/V03.06.0100/V03.05.0400/V03.05.0020;R5500G4V03.08.0100/V03.07.0200/V03.07.0100/V03.06.010	N/A	H-ZTE-R530-190820/1813

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			0> **CVE ID : CVE-2020-6871**		
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	20-Jul-20	4.3	The server management software module of ZTE has a storage XSS vulnerability. The attacker inserts some attack codes through the foreground login page, which will cause the user to execute the predefined malicious script in the browser. This affects <R5300G4V03.08.0100/V03.07.0300/V03.07.0200/V03.07.0108/V03.07.0100/V03.05.0047/V03.05.0046/V03.05.0045/V03.05.0044/V03.05.0043/V03.05.0040/V03.04.0020;R8500G4V03.07.0103/V03.07.0101/V03.06.0100/V03.05.0400/V03.05.0020;R5500G4V03.08.0100/V03.07.0200/V03.07.0100/V03.06.0100>. **CVE ID : CVE-2020-6872**	N/A	H-ZTE-R530-190820/1814