National Critical Information Infrastructure Protection Centre

Common Vulnerabilities and Exposures(CVE) Report

01 - 15 Oct 2020 Vol. 07 No. 19

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Application					
Apache					
ant					
Improper Neutralization of Special Elements in Output Used by a Downstream Component ('Injection')	01-Oct-20	5	As mitigation for CVE-2020-1945 Apache Ant 1.10.8 changed the permissions of temporary files it created so that only the current user was allowed to access them. Unfortunately the fixcrlf task deleted the temporary file and created a new one without said protection, effectively nullifying the effort. This would still allow an attacker to inject modified source files into the build process. **CVE ID : CVE-2020-11979**	N/A	A-APA-ANT-191020/1
nifi					
Improper Restriction of XML External Entity Reference ('XXE')	01-Oct-20	4.3	In Apache NiFi 1.0.0 to 1.11.4, the notification service manager and various policy authorizer and user group provider objects allowed trusted administrators to inadvertently configure a potentially malicious XML file. The XML file has the ability to make external calls to services (via XXE). **CVE ID : CVE-2020-13940**	N/A	A-APA-NIFI-191020/2

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
Information Exposure Through Log Files	01-Oct-20	5	In Apache NiFi 1.10.0 to 1.11.4, the NiFi stateless execution engine produced log output which included sensitive property values. When a flow was triggered, the flow definition configuration JSON was printed, potentially containing sensitive values in plaintext. **CVE ID : CVE-2020-9486**	N/A	A-APA-NIFI-191020/3
Missing Authentication for Critical Function	01-Oct-20	5	In Apache NiFi 1.0.0 to 1.11.4, the NiFi download token (one-time password) mechanism used a fixed cache size and did not authenticate a request to create a download token, only when attempting to use the token to access the content. An unauthenticated user could repeatedly request download tokens, preventing legitimate users from requesting download tokens. **CVE ID : CVE-2020-9487**	N/A	A-APA-NIFI-191020/4
Inadequate Encryption Strength	01-Oct-20	5	In Apache NiFi 1.2.0 to 1.11.4, the NiFi UI and API were protected by mandating TLS v1.2, as well as listening connections established by processors like ListenHTTP, HandleHttpRequest, etc.	N/A	A-APA-NIFI-191020/5

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			However intracluster communication such as cluster request replication, Site-to-Site, and load balanced queues continued to support TLS v1.0 or v1.1. **CVE ID : CVE-2020-9491**		
Artica					
pandora_fms					
Improper Neutralization of Special Elements used in an SQL Command ('SQL Injection')	02-Oct-20	7.5	Artica Pandora FMS before 743 allows unauthenticated attackers to conduct SQL injection attacks via the pandora_console/include/chart_generator.php session_id parameter. **CVE ID : CVE-2020-26518**	N/A	A-ART-PAND-191020/6
Artifex					
mupdf					
Out-of-bounds Write	02-Oct-20	4.3	Artifex MuPDF before 1.18.0 has a heap based buffer over-write when parsing JBIG2 files allowing attackers to cause a denial of service. **CVE ID : CVE-2020-26519**	N/A	A-ART-MUPD-191020/7
barchart					
maven_cascade_release					
Missing Authorization	08-Oct-20	4	Jenkins Maven Cascade Release Plugin 1.3.2 and earlier does not perform permission checks in several HTTP endpoints, allowing attackers with Overall/Read permission	https://www.jenkins.io/security/advisory/2020-10-08/#SECURITY-2049	A-BAR-MAVE-191020/8

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			to start cascade builds and layout builds, and reconfigure the plugin. **CVE ID : CVE-2020-2294**		
Cross-Site Request Forgery (CSRF)	08-Oct-20	4.3	A cross-site request forgery (CSRF) vulnerability in Jenkins Maven Cascade Release Plugin 1.3.2 and earlier allows attackers to start cascade builds and layout builds, and reconfigure the plugin. **CVE ID : CVE-2020-2295**	https://www.jenkins.io/security/advisory/2020-10-08/#SECURITY-2049	A-BAR-MAVE-191020/9
Bitdefender					
engines					
Out-of-bounds Write	01-Oct-20	5	A vulnerability has been discovered in the ace.xmd parser that results from a lack of proper validation of user-supplied data, which can result in a write past the end of an allocated buffer. This can result in denial-of-service. This issue affects: Bitdefender Engines version 7.84892 and prior versions. **CVE ID : CVE-2020-8109**	https://www.bitdefender.com/support/security-advisories/bitdefender-ace-xmd-parser-out-of-bounds-write-va-8772	A-BIT-ENGI-191020/10
Access of Uninitialized Pointer	02-Oct-20	5	A vulnerability has been discovered in the ceva_emu.cvd module that results from a lack of proper validation of user-supplied data, which can result in a pointer that is fetched from uninitialized memory. This can lead to denial-of-service. This	N/A	A-BIT-ENGI-191020/11

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			issue affects: Bitdefender Engines version 7.84897 and prior versions. **CVE ID : CVE-2020-8110**		
bludit					
bludit					
Improper Limitation of a Pathname to a Restricted Directory ('Path Traversal')	02-Oct-20	6.4	Bludit v3.8.1 is affected by directory traversal. Remote attackers are able to delete arbitrary files via /admin/ajax/upload-profile-picture. **CVE ID : CVE-2020-18190**	N/A	A-BLU-BLUD-191020/12
car_rental_management_system_project					
car_rental_management_system					
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	06-Oct-20	4.3	A Persistent Cross-Site Scripting (XSS) vulnerability in message_admin.php in Projectworlds Car Rental Management System v1.0 allows unauthenticated remote attackers to harvest an admin login session cookie and steal an admin session upon an admin login. **CVE ID : CVE-2020-23832**	N/A	A-CAR-CAR_-191020/13
clickstudios					
passwordstate					
Weak Password Recovery Mechanism for Forgotten Password	05-Oct-20	5	ClickStudios Passwordstate Password Reset Portal prior to build 8501 is affected by an authentication bypass vulnerability. The ResetPassword function	N/A	A-CLI-PASS-191020/14

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			does not validate whether the user has successfully authenticated using security questions. An unauthenticated, remote attacker can send a crafted HTTP request to the /account/ResetPassword page to set a new password for any registered user. **CVE ID : CVE-2020-26061**		
cloud_foundry					
bosh_system_metrics_server					
Exposure of Resource to Wrong Sphere	02-Oct-20	4	BOSH System Metrics Server releases prior to 0.1.0 exposed the UAA password as a flag to a process running on the BOSH director. It exposed the password to any user or process with access to the same VM (through ps or looking at process details). **CVE ID : CVE-2020-5422**	https://www.cloudfoundry.org/blog/cve-2020-5422	A-CLO-BOSH-191020/15
cloudflare					
cloudflared					
Improper Privilege Management	02-Oct-20	4.6	`cloudflared` versions prior to 2020.8.1 contain a local privilege escalation vulnerability on Windows systems. When run on a Windows system, `cloudflared` searches for configuration files which could be abused by a malicious entity to execute commands as a privileged	https://github.com/cloudflare/cloudflared/security/advisories/GHSA-hgwp-4vp4-qmm2	A-CLO-CLOU-191020/16

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			user. Version 2020.8.1 fixes this issue. **CVE ID : CVE-2020-24356**		
cmonos					
cmonos					
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	06-Oct-20	4.3	Stored cross-site scripting vulnerability in CMONOS.JP ver2.0.20191009 and earlier allows remote attackers to inject arbitrary script via unspecified vectors. **CVE ID : CVE-2020-5631**	N/A	A-CMO-CMON-191020/17
Cmsmadesimple					
cms_made_simple					
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	01-Oct-20	3.5	CMS Made Simple 2.2.14 allows an authenticated user with access to the Content Manager to edit content and put persistent XSS payload in the affected text fields. The user can get cookies from every authenticated user who visits the website. **CVE ID : CVE-2020-24860**	N/A	A-CMS-CMS_-191020/18
compass-security					
fusionauth-samlv2					
Improper Verification of Cryptographic Signature	02-Oct-20	6.4	FusionAuth fusionauth-samlv2 0.2.3 allows remote attackers to forge messages and bypass authentication via a SAML assertion that lacks a Signature element, aka a "Signature exclusion	N/A	A-COM-FUSI-191020/19

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			attack". **CVE ID : CVE-2020-12676**		
Craftercms					
studio					
Improper Control of Dynamically-Managed Code Resources	06-Oct-20	9	Improper Control of Dynamically-Managed Code Resources vulnerability in Crafter Studio of Crafter CMS allows authenticated developers to execute OS commands via Groovy scripting. This issue affects: Crafter Software Crafter CMS 3.0 versions prior to 3.0.27; 3.1 versions prior to 3.1.7. **CVE ID : CVE-2020-25802**	https://docs.craftercms.org/en/3.1/security/advisory.html#cv-2020080101	A-CRA-STUD-191020/20
Improper Control of Dynamically-Managed Code Resources	06-Oct-20	9	Improper Control of Dynamically-Managed Code Resources vulnerability in Crafter Studio of Crafter CMS allows authenticated developers to execute OS commands via FreeMarker template exposed objects. This issue affects: Crafter Software Crafter CMS 3.0 versions prior to 3.0.27; 3.1 versions prior to 3.1.7. **CVE ID : CVE-2020-25803**	N/A	A-CRA-STUD-191020/21
cuppacms					
cuppacms					
Unrestricted Upload of File with Dangerous	05-Oct-20	6.5	The file manager option in CuppaCMS before 2019-11-12 allows an authenticated attacker to	N/A	A-CUP-CUPP-191020/22

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Type			upload a malicious file within an image extension and through a custom request using the rename function provided by the file manager is able to modify the image extension into PHP resulting in remote arbitrary code execution. **CVE ID : CVE-2020-26048**		
damstratechnology					
smart_asset					
Improper Neutralization of Special Elements used in an SQL Command ('SQL Injection')	02-Oct-20	6.4	Damstra Smart Asset 2020.7 has SQL injection via the API/api/Asset originator parameter. This allows forcing the database and server to initiate remote connections to third party DNS servers. **CVE ID : CVE-2020-26525**	N/A	A-DAM-SMAR-191020/23
N/A	02-Oct-20	5	An issue was discovered in Damstra Smart Asset 2020.7. It is possible to enumerate valid usernames on the login page. The application sends a different server response when the username is invalid than when the username is valid ("Unable to find an APIDomain" versus "Wrong email or password"). **CVE ID : CVE-2020-26526**	N/A	A-DAM-SMAR-191020/24

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Origin Validation Error	02-Oct-20	7.5	An issue was discovered in API/api/Version in Damstra Smart Asset 2020.7. Cross-origin resource sharing trusts random origins by accepting the arbitrary 'Origin: example.com' header and responding with 200 OK and a wildcard 'Access-Control-Allow-Origin: *' header. **CVE ID : CVE-2020-26527**	N/A	A-DAM-SMAR-191020/25
envoyproxy					
envoy					
N/A	01-Oct-20	7.5	Envoy through 1.15.0 only considers the first value when multiple header values are present for some HTTP headers. Envoy's setCopy() header map API does not replace all existing occurences of a non-inline header. **CVE ID : CVE-2020-25017**	N/A	A-ENV-ENVO-191020/26
N/A	01-Oct-20	5	Envoy master between 2d69e30 and 3b5acb2 may fail to parse request URL that requires host canonicalization. **CVE ID : CVE-2020-25018**	N/A	A-ENV-ENVO-191020/27
Erlang					
erlang\/otp					
Improper Limitation of a Pathname to a Restricted Directory	02-Oct-20	4.3	Erlang/OTP 22.3.x before 22.3.4.6 and 23.x before 23.1 allows Directory Traversal. An attacker can send a crafted HTTP	https://github.com/erlang/otp/releases/tag/OTP-23.1,	A-ERL-ERLA-191020/28

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
('Path Traversal')			request to read arbitrary files, if httpd in the inets application is used. **CVE ID : CVE-2020-25623**	https://www.erlang.org/downloads	
Foxitsoftware					
foxit_reader					
Use After Free	02-Oct-20	7.5	An issue was discovered in Foxit Reader and PhantomPDF before 10.1. There is an Opt object use-after-free related to Field::ClearItems and Field::DeleteOptions, during AcroForm JavaScript execution. **CVE ID : CVE-2020-26534**	N/A	A-FOX-FOXI-191020/29
Out-of-bounds Write	02-Oct-20	7.5	An issue was discovered in Foxit Reader and PhantomPDF before 10.1. If TslAlloc attempts to allocate thread local storage but obtains an unacceptable index value, V8 throws an exception that leads to a write access violation (and read access violation). **CVE ID : CVE-2020-26535**	N/A	A-FOX-FOXI-191020/30
NULL Pointer Dereference	02-Oct-20	4.3	An issue was discovered in Foxit Reader and PhantomPDF before 10.1. There is a NULL pointer dereference via a crafted PDF document. **CVE ID : CVE-2020-26536**	N/A	A-FOX-FOXI-191020/31
Out-of-bounds Write	02-Oct-20	7.5	An issue was discovered in Foxit Reader and PhantomPDF before 10.1.	N/A	A-FOX-FOXI-191020/32

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			In a certain Shading calculation, the number of outputs is unequal to the number of color components in a color space. This causes an out-of-bounds write. **CVE ID : CVE-2020-26537**		
N/A	02-Oct-20	4.4	An issue was discovered in Foxit Reader and PhantomPDF before 10.1. It allows attackers to execute arbitrary code via a Trojan horse taskkill.exe in the current working directory. **CVE ID : CVE-2020-26538**	N/A	A-FOX-FOXI-191020/33
Use After Free	02-Oct-20	7.5	An issue was discovered in Foxit Reader and PhantomPDF before 10.1. When there is a multiple interpretation error for /V (in the Additional Action and Field dictionaries), a use-after-free can occur with resultant remote code execution (or an information leak). **CVE ID : CVE-2020-26539**	N/A	A-FOX-FOXI-191020/34
Improper Control of Generation of Code ('Code Injection')	02-Oct-20	5	An issue was discovered in Foxit Reader and PhantomPDF before 4.1 on macOS. Because the Hardened Runtime protection mechanism is not applied to code signing, code injection (or an information leak) can occur.	N/A	A-FOX-FOXI-191020/35

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2020-26540		
phantompdf					
Use After Free	02-Oct-20	7.5	An issue was discovered in Foxit Reader and PhantomPDF before 10.1. There is an Opt object use-after-free related to Field::ClearItems and Field::DeleteOptions, during AcroForm JavaScript execution. **CVE ID : CVE-2020-26534**	N/A	A-FOX-PHAN-191020/36
Out-of-bounds Write	02-Oct-20	7.5	An issue was discovered in Foxit Reader and PhantomPDF before 10.1. If TslAlloc attempts to allocate thread local storage but obtains an unacceptable index value, V8 throws an exception that leads to a write access violation (and read access violation). **CVE ID : CVE-2020-26535**	N/A	A-FOX-PHAN-191020/37
NULL Pointer Dereference	02-Oct-20	4.3	An issue was discovered in Foxit Reader and PhantomPDF before 10.1. There is a NULL pointer dereference via a crafted PDF document. **CVE ID : CVE-2020-26536**	N/A	A-FOX-PHAN-191020/38
Out-of-bounds Write	02-Oct-20	7.5	An issue was discovered in Foxit Reader and PhantomPDF before 10.1. In a certain Shading calculation, the number of outputs is unequal to the number of color components in a color	N/A	A-FOX-PHAN-191020/39

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			space. This causes an out-of-bounds write. **CVE ID : CVE-2020-26537**		
N/A	02-Oct-20	4.4	An issue was discovered in Foxit Reader and PhantomPDF before 10.1. It allows attackers to execute arbitrary code via a Trojan horse taskkill.exe in the current working directory. **CVE ID : CVE-2020-26538**	N/A	A-FOX-PHAN-191020/40
Use After Free	02-Oct-20	7.5	An issue was discovered in Foxit Reader and PhantomPDF before 10.1. When there is a multiple interpretation error for /V (in the Additional Action and Field dictionaries), a use-after-free can occur with resultant remote code execution (or an information leak). **CVE ID : CVE-2020-26539**	N/A	A-FOX-PHAN-191020/41
Improper Control of Generation of Code ('Code Injection')	02-Oct-20	5	An issue was discovered in Foxit Reader and PhantomPDF before 4.1 on macOS. Because the Hardened Runtime protection mechanism is not applied to code signing, code injection (or an information leak) can occur. **CVE ID : CVE-2020-26540**	N/A	A-FOX-PHAN-191020/42
froala					
froala_editor					
Improper	02-Oct-20	4.3	Froala Editor before 3.2.2	N/A	A-FRO-

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Neutralization of Input During Web Page Generation ('Cross-site Scripting')			allows XSS via pasted content. **CVE ID : CVE-2020-26523**		FROA-191020/43
getfilecloud					
filecloud					
Information Exposure	02-Oct-20	5	CodeLathe FileCloud before 20.2.0.11915 allows username enumeration. **CVE ID : CVE-2020-26524**	N/A	A-GET-FILE-191020/44
Get-simple					
getsimplecms					
Improper Limitation of a Pathname to a Restricted Directory ('Path Traversal')	02-Oct-20	6.4	GetSimpleCMS-3.3.15 is affected by directory traversal. Remote attackers are able to delete arbitrary files via /GetSimpleCMS-3.3.15/admin/log.php **CVE ID : CVE-2020-18191**	N/A	A-GET-GETS-191020/45
getsimple_cms					
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	01-Oct-20	3.5	GetSimple CMS 3.3.16 allows in parameter 'permalink' on the Settings page persistent Cross Site Scripting which is executed when you create and open a new page **CVE ID : CVE-2020-24861**	N/A	A-GET-GETS-191020/46
Getsymphony					
symphony					
Improper Neutralization of Input During Web Page	07-Oct-20	3.5	Cross-site scripting (XSS) vulnerabilities in Symphony CMS 3.0.0 allow remote attackers to inject	N/A	A-GET-SYMP-191020/47

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Generation ('Cross-site Scripting')			arbitrary web script or HTML to fields['body'] param via events\event.publish_article.php **CVE ID : CVE-2020-25343**		
Gitlab					
gitlab					
Uncontrolled Resource Consumption	06-Oct-20	4	A potential DOS vulnerability was discovered in GitLab versions 13.1, 13.2 and 13.3. The api to update an asset as a link from a release had a regex check which caused exponential number of backtracks for certain user supplied values resulting in high CPU usage. **CVE ID : CVE-2020-13333**	https://gitlab.com/gitlab-org/cves/-/blob/master/2020/CVE-2020-13333.json	A-GIT-GITL-191020/48
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	02-Oct-20	3.5	An issue has been discovered in GitLab affecting versions from 12.10 to 12.10.12 that allowed for a stored XSS payload to be added as a group name. **CVE ID : CVE-2020-13337**	https://gitlab.com/gitlab-org/cves/-/blob/master/2020/CVE-2020-13337.json	A-GIT-GITL-191020/49
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	02-Oct-20	3.5	An issue has been discovered in GitLab affecting versions prior to 12.10.13, 13.0.8, 13.1.2. A stored cross-site scripting vulnerability was discovered when editing references. **CVE ID : CVE-2020-13338**	https://gitlab.com/gitlab-org/cves/-/blob/master/2020/CVE-2020-13338.json	A-GIT-GITL-191020/50

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	08-Oct-20	6	An issue has been discovered in GitLab affecting all versions before 13.2.10, 13.3.7 and 13.4.2: XSS in SVG File Preview. Overall impact is limited due to the current user only being impacted. **CVE ID : CVE-2020-13339**	https://gitlab.com/gitlab-org/cves/-/blob/master/2020/CVE-2020-13339.json	A-GIT-GITL-191020/51
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	08-Oct-20	3.5	An issue has been discovered in GitLab affecting all versions prior to 13.2.10, 13.3.7 and 13.4.2: Stored XSS in CI Job Log **CVE ID : CVE-2020-13340**	https://gitlab.com/gitlab-org/cves/-/blob/master/2020/CVE-2020-13340.json	A-GIT-GITL-191020/52
Exposure of Resource to Wrong Sphere	06-Oct-20	4	An issue has been discovered in GitLab affecting all versions starting from 11.2. Unauthorized Users Can View Custom Project Template **CVE ID : CVE-2020-13343**	https://gitlab.com/gitlab-org/cves/-/blob/master/2020/CVE-2020-13343.json	A-GIT-GITL-191020/53
Glpi-project					
glpi					
Improper Neutralization of Special Elements used in an SQL Command ('SQL Injection')	07-Oct-20	5	In GLPI before version 9.5.2, there is a SQL Injection in the API's search function. Not only is it possible to break the SQL syntax, but it is also possible to utilise a UNION SELECT query to reflect sensitive information such as the current database version, or database user. The most likely scenario for this vulnerability is	https://github.com/glpi-project/glpi/commit/3dc4475c56b241ad659cc5c7cb5fb65727409cf0, https://github.com/glpi-project/glpi/security/advisories/GHSA	A-GLP-GLPI-191020/54

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			with someone who has an API account to the system. The issue is patched in version 9.5.2. A proof-of-concept with technical details is available in the linked advisory. **CVE ID : CVE-2020-15226**	-jwpv-7m4h-5gvc	
hcltech					
digital_experience					
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	01-Oct-20	4.3	HCL Digital Experience 8.5, 9.0, 9.5 is susceptible to cross-site scripting (XSS). The vulnerability could be employed in a reflected or non-persistent XSS attack. **CVE ID : CVE-2020-14223**	N/A	A-HCL-DIGI-191020/55
IBM					
informix_dynamic_server					
Out-of-bounds Write	08-Oct-20	4.6	IBM Informix spatial 14.10 could allow a local user to execute commands as a privileged user due to an out of bounds write vulnerability. IBM X-Force ID: 189460. **CVE ID : CVE-2020-4799**	https://www.ibm.com/support/pages/node/6343587	A-IBM-INFO-191020/56
security_guardium					
Improper Neutralization of Special Elements in Output Used by a Downstream Component ('Injection')	12-Oct-20	8.5	IBM Security Guardium 11.2 is vulnerable to CVS Injection. A remote privileged attacker could execute arbitrary commands on the system, caused by improper validation of csv file contents. IBM X-ForceID:	https://www.ibm.com/support/pages/node/6346884	A-IBM-SECU-191020/57

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			186696. **CVE ID : CVE-2020-4689**		
Information Exposure	12-Oct-20	4	IBM Security Guardium 11.2 could allow an attacker with admin access to obtain and read files that they normally would not have access to. IBM X-Force ID: 186423. **CVE ID : CVE-2020-4678**	https://www.ibm.com/support/pages/node/6346884	A-IBM-SECU-191020/58
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	12-Oct-20	3.5	IBM Security Guardium 11.2 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: 186424. **CVE ID : CVE-2020-4679**	https://www.ibm.com/support/pages/node/6346884	A-IBM-SECU-191020/59
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	12-Oct-20	3.5	IBM Security Guardium 11.2 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: 186426. **CVE ID : CVE-2020-4680**	https://www.ibm.com/support/pages/node/6346884	A-IBM-SECU-191020/60
Improper Neutralization of Input During	12-Oct-20	3.5	IBM Security Guardium 11.2 is vulnerable to cross-site scripting. This	https://www.ibm.com/support/page	A-IBM-SECU-191020/61

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Web Page Generation ('Cross-site Scripting')			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: 186427. **CVE ID : CVE-2020-4681**	s/node/6346884	
datapower_gateway					
Information Exposure	06-Oct-20	1.9	IBM MQ Appliance (IBM DataPower Gateway 10.0.0.0 and 2018.4.1.0 through 2018.4.1.12) could allow a local user, under special conditions, to obtain highly sensitive information from log files. IBM X-Force ID: 182658. **CVE ID : CVE-2020-4528**	https://www.ibm.com/support/pages/node/6333033	A-IBM-DATA-191020/62
cognos_analytics					
Improper Handling of Exceptional Conditions	12-Oct-20	9.3	IBM Cognos Analytics 11.0 and 11.1 could allow a remote attacker to execute arbitrary code on the system, caused by a CSV injection. By persuading a victim to open a specially-crafted excel file, an attacker could exploit this vulnerability to execute arbitrary code on the system. IBM X-Force ID: 176610. **CVE ID : CVE-2020-4302**	https://www.ibm.com/support/pages/node/6346922	A-IBM-COGN-191020/63
Improper Handling of Exceptional	12-Oct-20	6.4	IBM Cognos Analytics 11.0 and 11.1 could be vulnerable to a denial of	https://www.ibm.com/support/page	A-IBM-COGN-

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Conditions			service attack by failing to catch exceptions in a servlet also exposing debug information could also be used in future attacks. IBM X-Force ID: 179270. **CVE ID : CVE-2020-4388**	s/node/6346922	191020/64
websphere_application_server					
N/A	01-Oct-20	5	IBM WebSphere Application Server 7.5, 8.0, 8.5, and 9.0 traditional could allow a remote attacker to obtain sensitive information with a specially-crafted sequence of serialized objects. IBM X-Force ID: 184428. **CVE ID : CVE-2020-4576**	https://www.ibm.com/support/pages/node/6339807	A-IBM-WEBS-191020/65
maximo_asset_management					
Improper Authentication	05-Oct-20	7.5	IBM Maximo Asset Management 7.6.0 and 7.6.1 could allow an attacker to bypass authentication and issue commands using a specially crafted HTTP command. IBM X-Force ID: 181995. **CVE ID : CVE-2020-4493**	https://www.ibm.com/support/pages/node/6340281	A-IBM-MAXI-191020/66
infosphere_information_server					
Improper Neutralization of Special Elements in Output Used by a Downstream Component	12-Oct-20	4.3	IBM InfoSphere Information Server 11.5 and 11.7 is vulnerable to HTML injection. A remote attacker could inject malicious HTML code, which when viewed,	https://www.ibm.com/support/pages/node/6346920	A-IBM-INFO-191020/67

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
('Injection')			would be executed in the victim's Web browser within the security context of the hosting site. IBM X-Force ID: 188150. **CVE ID : CVE-2020-4740**		
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	12-Oct-20	3.5	IBM InfoSphere Information Server 11.5 and 11.7 is vulnerable to stored cross-site scripting. This vulnerability allows users to embed arbitrary JavaScript code in the Web UI thus altering the intended functionality potentially leading to credentials disclosure within a trusted session. IBM X-Force ID: 188197. **CVE ID : CVE-2020-4741**	https://www.ibm.com/support/pages/node/6346906	A-IBM-INFO-191020/68
Impresscms					
impresscms					
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	07-Oct-20	3.5	ImpressCMS 1.4.0 is affected by XSS in modules/system/admin.php which may result in arbitrary remote code execution. **CVE ID : CVE-2020-17551**	N/A	A-IMP-IMPR-191020/69
Intel					
driver_\&_support_assistant					
Improper Privilege Management	05-Oct-20	4.6	Improper permissions in the Intel(R) Driver & Support Assistant before version 20.7.26.7 may allow an authenticated user to potentially enable escalation of privilege via	N/A	A-INT-DRIV-191020/70

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			local access. **CVE ID : CVE-2020-12302**		
istio					
istio					
N/A	01-Oct-20	5.5	In Istio 1.5.0 though 1.5.8 and Istio 1.6.0 through 1.6.7, when users specify an AuthorizationPolicy resource with DENY actions using wildcard suffixes (e.g. *-some-suffix) for source principals or namespace fields, callers will never be denied access, bypassing the intended policy. **CVE ID : CVE-2020-16844**	https://istio.io/latest/news/security/istio-security-2020-009/	A-IST-ISTI-191020/71
Jenkins					
active_choices					
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	08-Oct-20	3.5	Jenkins Active Choices Plugin 2.4 and earlier does not escape the name and description of build parameters, resulting in a stored cross-site scripting (XSS) vulnerability exploitable by attackers with Job/Configure permission. **CVE ID : CVE-2020-2289**	https://www.jenkins.io/security/advisory/2020-10-08/#SECURITY-1954	A-JEN-ACTI-191020/72
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	08-Oct-20	3.5	Jenkins Active Choices Plugin 2.4 and earlier does not escape some return values of sandboxed scripts for Reactive Reference Parameters, resulting in a stored cross-site scripting (XSS)	https://www.jenkins.io/security/advisory/2020-10-08/#SECURITY-2008	A-JEN-ACTI-191020/73

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			vulnerability exploitable by attackers with Job/Configure permission. **CVE ID : CVE-2020-2290**		
couchdb-statistics					
Unprotected Storage of Credentials	08-Oct-20	2.1	Jenkins couchdb-statistics Plugin 0.3 and earlier stores its server password unencrypted in its global configuration file on the Jenkins controller where it can be viewed by users with access to the Jenkins controller file system. **CVE ID : CVE-2020-2291**	https://www.jenkins.io/security/advisory/2020-10-08/#SECURITY-2065	A-JEN-COUC-191020/74
persona					
Improper Limitation of a Pathname to a Restricted Directory ('Path Traversal')	08-Oct-20	4	Jenkins Persona Plugin 2.4 and earlier allows users with Overall/Read permission to read arbitrary files on the Jenkins controller. **CVE ID : CVE-2020-2293**	https://www.jenkins.io/security/advisory/2020-10-08/#SECURITY-2046	A-JEN-PERS-191020/75
shared_objects					
Cross-Site Request Forgery (CSRF)	08-Oct-20	4.3	A cross-site request forgery (CSRF) vulnerability in Jenkins Shared Objects Plugin 0.44 and earlier allows attackers to configure shared objects. **CVE ID : CVE-2020-2296**	https://www.jenkins.io/security/advisory/2020-10-08/#SECURITY-2052	A-JEN-SHAR-191020/76
audit_trail					
Incorrect Regular Expression	08-Oct-20	5	In Jenkins Audit Trail Plugin 3.6 and earlier, the default regular expression pattern could be bypassed	https://www.jenkins.io/security/advisory/2020-	A-JEN-AUDI-191020/77

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			in many cases by adding a suffix to the URL that would be ignored during request handling. **CVE ID : CVE-2020-2288**	10-08/#SECURITY-1846	
livehelperchat					
live_helper_chat					
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	02-Oct-20	4.3	Live Helper Chat before 3.44v allows stored XSS in chat messages with an operator via BBCode. **CVE ID : CVE-2020-26134**	N/A	A-LIV-LIVE-191020/78
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	02-Oct-20	4.3	Live Helper Chat before 3.44v allows reflected XSS via the setsettingajax PATH_INFO. **CVE ID : CVE-2020-26135**	N/A	A-LIV-LIVE-191020/79
mapfish					
print					
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	02-Oct-20	4.3	In mapfish-print before version 3.24, a user can use the JSONP support to do a Cross-site scripting. **CVE ID : CVE-2020-15231**	https://github.com/mapfish/mapfish-print/security/advisories/GHSA-w534-q4xf-h5v2	A-MAP-PRIN-191020/80
Improper Restriction of XML External Entity Reference ('XXE')	02-Oct-20	6.4	In mapfish-print before version 3.24, a user can do to an XML External Entity (XXE) attack with the provided SDL style. **CVE ID : CVE-2020-15232**	https://github.com/mapfish/mapfish-print/security/advisories/GHSA-vjv6-gq77-3mjw	A-MAP-PRIN-191020/81

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
monocms					
monocms					
Improper Limitation of a Pathname to a Restricted Directory ('Path Traversal')	07-Oct-20	5.5	MonoCMS Blog 1.0 is affected by: Arbitrary File Deletion. Any authenticated user can delete files on and off the webserver (php files can be unlinked and not deleted). **CVE ID : CVE-2020-25985**	N/A	A-MON-MONO-191020/82
Cross-Site Request Forgery (CSRF)	06-Oct-20	4.3	A Cross Site Request Forgery (CSRF) vulnerability in MonoCMS Blog 1.0 allows attackers to change the password of a user. **CVE ID : CVE-2020-25986**	N/A	A-MON-MONO-191020/83
Information Exposure Through Log Files	06-Oct-20	5	MonoCMS Blog 1.0 stores hard-coded admin hashes in the log.xml file in the source files for MonoCMS Blog. Hash type is bcrypt and hashcat mode 3200 can be used to crack the hash. **CVE ID : CVE-2020-25987**	N/A	A-MON-MONO-191020/84
Mozilla					
firefox					
Improper Privilege Management	01-Oct-20	9.3	If Firefox is installed to a user-writable directory, the Mozilla Maintenance Service would execute updater.exe from the install location with system privileges. Although the Mozilla Maintenance Service does	N/A	A-MOZ-FIRE-191020/85

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			ensure that updater.exe is signed by Mozilla, the version could have been rolled back to a previous version which would have allowed exploitation of an older bug and arbitrary code execution with System Privileges. *Note: This issue only affected Windows operating systems. Other operating systems are unaffected.*. This vulnerability affects Firefox < 80, Thunderbird < 78.2, Thunderbird < 68.12, Firefox ESR < 68.12, and Firefox ESR < 78.2. **CVE ID : CVE-2020-15663**		
Incorrect Authorization	01-Oct-20	4.3	By holding a reference to the eval() function from an about:blank window, a malicious webpage could have gained access to the InstallTrigger object which would allow them to prompt the user to install an extension. Combined with user confusion, this could result in an unintended or malicious extension being installed. This vulnerability affects Firefox < 80, Thunderbird < 78.2, Thunderbird < 68.12, Firefox ESR < 68.12, Firefox ESR < 78.2, and Firefox for Android < 80. **CVE ID : CVE-2020-15664**	N/A	A-MOZ-FIRE-191020/86
N/A	01-Oct-20	4.3	Firefox did not reset the	N/A	A-MOZ-

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			address bar after the beforeunload dialog was shown if the user chose to remain on the page. This could have resulted in an incorrect URL being shown when used in conjunction with other unexpected browser behaviors. This vulnerability affects Firefox < 80. **CVE ID : CVE-2020-15665**		FIRE-191020/87
Information Exposure	01-Oct-20	4.3	When trying to load a non-video in an audio/video context the exact status code (200, 302, 404, 500, 412, 403, etc.) was disclosed via the MediaError Message. This level of information leakage is inconsistent with the standardized onerror/onsuccess disclosure and can lead to inferring login status to services or device discovery on a local network among other attacks. This vulnerability affects Firefox < 80 and Firefox for Android < 80. **CVE ID : CVE-2020-15666**	N/A	A-MOZ-FIRE-191020/88
Unrestricted Upload of File with Dangerous Type	01-Oct-20	6.8	When processing a MAR update file, after the signature has been validated, an invalid name length could result in a heap overflow, leading to memory corruption and potentially arbitrary code	N/A	A-MOZ-FIRE-191020/89

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			execution. Within Firefox as released by Mozilla, this issue is only exploitable with the Mozilla-controlled signing key. This vulnerability affects Firefox < 80. **CVE ID : CVE-2020-15667**		
Improper Locking	01-Oct-20	4.3	A lock was missing when accessing a data structure and importing certificate information into the trust database. This vulnerability affects Firefox < 80 and Firefox for Android < 80. **CVE ID : CVE-2020-15668**	N/A	A-MOZ-FIRE-191020/90
Release of Invalid Pointer or Reference	01-Oct-20	6.8	Mozilla developers reported memory safety bugs present in Firefox for Android 79. Some of these bugs showed evidence of memory corruption and we presume that with enough effort some of these could have been exploited to run arbitrary code. This vulnerability affects Firefox < 80, Firefox ESR < 78.2, Thunderbird < 78.2, and Firefox for Android < 80. **CVE ID : CVE-2020-15670**	N/A	A-MOZ-FIRE-191020/91
Improper Input Validation	01-Oct-20	2.6	When typing in a password under certain conditions, a race may have occured where the InputContext was not being correctly set for the	N/A	A-MOZ-FIRE-191020/92

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			input field, resulting in the typed password being saved to the keyboard dictionary. This vulnerability affects Firefox for Android < 80. **CVE ID : CVE-2020-15671**		
Release of Invalid Pointer or Reference	01-Oct-20	6.8	Mozilla developers reported memory safety bugs present in Firefox 80 and Firefox ESR 78.2. Some of these bugs showed evidence of memory corruption and we presume that with enough effort some of these could have been exploited to run arbitrary code. This vulnerability affects Firefox < 81, Thunderbird < 78.3, and Firefox ESR < 78.3. **CVE ID : CVE-2020-15673**	N/A	A-MOZ-FIRE-191020/93
Release of Invalid Pointer or Reference	01-Oct-20	6.8	Mozilla developers reported memory safety bugs present in Firefox 80. Some of these bugs showed evidence of memory corruption and we presume that with enough effort some of these could have been exploited to run arbitrary code. This vulnerability affects Firefox < 81. **CVE ID : CVE-2020-15674**	N/A	A-MOZ-FIRE-191020/94
Buffer Copy without Checking Size	01-Oct-20	6.8	When processing surfaces, the lifetime may outlive a persistent buffer leading to	N/A	A-MOZ-FIRE-191020/95

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
of Input ('Classic Buffer Overflow')			memory corruption and a potentially exploitable crash. This vulnerability affects Firefox < 81. **CVE ID : CVE-2020-15675**		
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	01-Oct-20	4.3	Firefox sometimes ran the onload handler for SVG elements that the DOM sanitizer decided to remove, resulting in JavaScript being executed after pasting attacker-controlled data into a contenteditable element. This vulnerability affects Firefox < 81, Thunderbird < 78.3, and Firefox ESR < 78.3. **CVE ID : CVE-2020-15676**	N/A	A-MOZ-FIRE-191020/96
URL Redirection to Untrusted Site ('Open Redirect')	01-Oct-20	5.8	By exploiting an Open Redirect vulnerability on a website, an attacker could have spoofed the site displayed in the download file dialog to show the original site (the one suffering from the open redirect) rather than the site the file was actually downloaded from. This vulnerability affects Firefox < 81, Thunderbird < 78.3, and Firefox ESR < 78.3. **CVE ID : CVE-2020-15677**	N/A	A-MOZ-FIRE-191020/97
Use After Free	01-Oct-20	6.8	When recursing through graphical layers while scrolling, an iterator may have become invalid,	N/A	A-MOZ-FIRE-191020/98

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			resulting in a potential use-after-free. This occurs because the function APZCTreeManager::ComputeClippedCompositionBounds did not follow iterator invalidation rules. This vulnerability affects Firefox < 81, Thunderbird < 78.3, and Firefox ESR < 78.3. **CVE ID : CVE-2020-15678**		
firefox_esr					
Improper Privilege Management	01-Oct-20	9.3	If Firefox is installed to a user-writable directory, the Mozilla Maintenance Service would execute updater.exe from the install location with system privileges. Although the Mozilla Maintenance Service does ensure that updater.exe is signed by Mozilla, the version could have been rolled back to a previous version which would have allowed exploitation of an older bug and arbitrary code execution with System Privileges. *Note: This issue only affected Windows operating systems. Other operating systems are unaffected.*. This vulnerability affects Firefox < 80, Thunderbird < 78.2, Thunderbird < 68.12, Firefox ESR < 68.12, and Firefox ESR < 78.2.	N/A	A-MOZ-FIRE-191020/99

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2020-15663		
Incorrect Authorization	01-Oct-20	4.3	By holding a reference to the eval() function from an about:blank window, a malicious webpage could have gained access to the InstallTrigger object which would allow them to prompt the user to install an extension. Combined with user confusion, this could result in an unintended or malicious extension being installed. This vulnerability affects Firefox < 80, Thunderbird < 78.2, Thunderbird < 68.12, Firefox ESR < 68.12, Firefox ESR < 78.2, and Firefox for Android < 80. **CVE ID : CVE-2020-15664**	N/A	A-MOZ-FIRE-191020/100
Use After Free	01-Oct-20	6.8	When aborting an operation, such as a fetch, an abort signal may be deleted while alerting the objects to be notified. This results in a use-after-free and we presume that with enough effort it could have been exploited to run arbitrary code. This vulnerability affects Firefox ESR < 68.12 and Thunderbird < 68.12. **CVE ID : CVE-2020-15669**	N/A	A-MOZ-FIRE-191020/101
Release of Invalid Pointer or Reference	01-Oct-20	6.8	Mozilla developers reported memory safety bugs present in Firefox for Android 79. Some of these bugs showed evidence of	N/A	A-MOZ-FIRE-191020/102

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			memory corruption and we presume that with enough effort some of these could have been exploited to run arbitrary code. This vulnerability affects Firefox < 80, Firefox ESR < 78.2, Thunderbird < 78.2, and Firefox for Android < 80. **CVE ID : CVE-2020-15670**		
Release of Invalid Pointer or Reference	01-Oct-20	6.8	Mozilla developers reported memory safety bugs present in Firefox 80 and Firefox ESR 78.2. Some of these bugs showed evidence of memory corruption and we presume that with enough effort some of these could have been exploited to run arbitrary code. This vulnerability affects Firefox < 81, Thunderbird < 78.3, and Firefox ESR < 78.3. **CVE ID : CVE-2020-15673**	N/A	A-MOZ-FIRE-191020/103
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	01-Oct-20	4.3	Firefox sometimes ran the onload handler for SVG elements that the DOM sanitizer decided to remove, resulting in JavaScript being executed after pasting attacker-controlled data into a contenteditable element. This vulnerability affects Firefox < 81, Thunderbird < 78.3, and Firefox ESR < 78.3.	N/A	A-MOZ-FIRE-191020/104

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2020-15676		
URL Redirection to Untrusted Site ('Open Redirect')	01-Oct-20	5.8	By exploiting an Open Redirect vulnerability on a website, an attacker could have spoofed the site displayed in the download file dialog to show the original site (the one suffering from the open redirect) rather than the site the file was actually downloaded from. This vulnerability affects Firefox < 81, Thunderbird < 78.3, and Firefox ESR < 78.3. **CVE ID : CVE-2020-15677**	N/A	A-MOZ-FIRE-191020/105
Use After Free	01-Oct-20	6.8	When recursing through graphical layers while scrolling, an iterator may have become invalid, resulting in a potential use-after-free. This occurs because the function APZCTreeManager::ComputeClippedCompositionBounds did not follow iterator invalidation rules. This vulnerability affects Firefox < 81, Thunderbird < 78.3, and Firefox ESR < 78.3. **CVE ID : CVE-2020-15678**	N/A	A-MOZ-FIRE-191020/106
thunderbird					
Improper Privilege Management	01-Oct-20	9.3	If Firefox is installed to a user-writable directory, the Mozilla Maintenance Service would execute updater.exe from the	N/A	A-MOZ-THUN-191020/107

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			install location with system privileges. Although the Mozilla Maintenance Service does ensure that updater.exe is signed by Mozilla, the version could have been rolled back to a previous version which would have allowed exploitation of an older bug and arbitrary code execution with System Privileges. *Note: This issue only affected Windows operating systems. Other operating systems are unaffected.*. This vulnerability affects Firefox < 80, Thunderbird < 78.2, Thunderbird < 68.12, Firefox ESR < 68.12, and Firefox ESR < 78.2. **CVE ID : CVE-2020-15663**		
Incorrect Authorization	01-Oct-20	4.3	By holding a reference to the eval() function from an about:blank window, a malicious webpage could have gained access to the InstallTrigger object which would allow them to prompt the user to install an extension. Combined with user confusion, this could result in an unintended or malicious extension being installed. This vulnerability affects Firefox < 80, Thunderbird < 78.2, Thunderbird < 68.12, Firefox ESR < 68.12, Firefox ESR < 78.2, and	N/A	A-MOZ-THUN-191020/108

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Firefox for Android < 80. **CVE ID : CVE-2020-15664**		
Use After Free	01-Oct-20	6.8	When aborting an operation, such as a fetch, an abort signal may be deleted while alerting the objects to be notified. This results in a use-after-free and we presume that with enough effort it could have been exploited to run arbitrary code. This vulnerability affects Firefox ESR < 68.12 and Thunderbird < 68.12. **CVE ID : CVE-2020-15669**	N/A	A-MOZ-THUN-191020/109
Release of Invalid Pointer or Reference	01-Oct-20	6.8	Mozilla developers reported memory safety bugs present in Firefox for Android 79. Some of these bugs showed evidence of memory corruption and we presume that with enough effort some of these could have been exploited to run arbitrary code. This vulnerability affects Firefox < 80, Firefox ESR < 78.2, Thunderbird < 78.2, and Firefox for Android < 80. **CVE ID : CVE-2020-15670**	N/A	A-MOZ-THUN-191020/110
Release of Invalid Pointer or Reference	01-Oct-20	6.8	Mozilla developers reported memory safety bugs present in Firefox 80 and Firefox ESR 78.2. Some of these bugs showed evidence of memory corruption and	N/A	A-MOZ-THUN-191020/111

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			we presume that with enough effort some of these could have been exploited to run arbitrary code. This vulnerability affects Firefox < 81, Thunderbird < 78.3, and Firefox ESR < 78.3. **CVE ID : CVE-2020-15673**		
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	01-Oct-20	4.3	Firefox sometimes ran the onload handler for SVG elements that the DOM sanitizer decided to remove, resulting in JavaScript being executed after pasting attacker-controlled data into a contenteditable element. This vulnerability affects Firefox < 81, Thunderbird < 78.3, and Firefox ESR < 78.3. **CVE ID : CVE-2020-15676**	N/A	A-MOZ-THUN-191020/112
URL Redirection to Untrusted Site ('Open Redirect')	01-Oct-20	5.8	By exploiting an Open Redirect vulnerability on a website, an attacker could have spoofed the site displayed in the download file dialog to show the original site (the one suffering from the open redirect) rather than the site the file was actually downloaded from. This vulnerability affects Firefox < 81, Thunderbird < 78.3, and Firefox ESR < 78.3. **CVE ID : CVE-2020-15677**	N/A	A-MOZ-THUN-191020/113

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Use After Free	01-Oct-20	6.8	When recursing through graphical layers while scrolling, an iterator may have become invalid, resulting in a potential use-after-free. This occurs because the function APZCTreeManager::ComputeClippedCompositionBounds did not follow iterator invalidation rules. This vulnerability affects Firefox < 81, Thunderbird < 78.3, and Firefox ESR < 78.3. **CVE ID : CVE-2020-15678**	N/A	A-MOZ-THUN-191020/114
mpd_project					
mpd					
Out-of-bounds Write	06-Oct-20	7.5	The L2TP implementation of MPD before 5.9 allows a remote attacker who can send specifically crafted L2TP control packet with AVP Q.931 Cause Code to execute arbitrary code or cause a denial of service (memory corruption). **CVE ID : CVE-2020-7465**	N/A	A-MPD-MPD-191020/115
Out-of-bounds Read	06-Oct-20	5	The PPP implementation of MPD before 5.9 allows a remote attacker who can send specifically crafted PPP authentication message to cause the daemon to read beyond allocated memory buffer, which would result in a denial of service condition. **CVE ID : CVE-2020-7466**	N/A	A-MPD-MPD-191020/116

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Nextcloud					
nextcloud_server					
Improper Privilege Management	05-Oct-20	3.5	A logic error in Nextcloud Server 19.0.0 caused a privilege escalation allowing malicious users to reshare with higher permissions than they got assigned themselves. **CVE ID : CVE-2020-8223**	N/A	A-NEX-NEXT-191020/117
deck					
Improper Preservation of Permissions	05-Oct-20	6	Improper access control in Nextcloud Deck 0.8.0 allowed an attacker to reshare boards shared with them with more permissions than they had themselves. **CVE ID : CVE-2020-8182**	N/A	A-NEX-DECK-191020/118
Authorization Bypass Through User-Controlled Key	05-Oct-20	4	Missing access control in Nextcloud Deck 1.0.4 caused an insecure direct object reference allowing an attacker to view all attachments. **CVE ID : CVE-2020-8235**	N/A	A-NEX-DECK-191020/119
Nvidia					
virtual_gpu_manager					
N/A	02-Oct-20	4.6	NVIDIA Windows GPU Display Driver, all versions, contains a vulnerability in the NVIDIA Control Panel component in which a user is presented with a dialog box for input by a high-privilege process, which may lead to escalation of	https://nvidia.custhelp.com/app/answers/detail/a_id/5075	A-NVI-VIRT-191020/120

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			privileges. **CVE ID : CVE-2020-5979**		
N/A	02-Oct-20	4.6	NVIDIA Windows GPU Display Driver, all versions, contains a vulnerability in multiple components in which a securely loaded system DLL will load its dependencies in an insecure fashion, which may lead to code execution or denial of service. **CVE ID : CVE-2020-5980**	https://nvidia.custhelp.com/app/answers/detail/a_id/5075	A-NVI-VIRT-191020/121
Out-of-bounds Write	02-Oct-20	4.6	NVIDIA Windows GPU Display Driver, all versions, contains a vulnerability in the DirectX11 user mode driver (nvwgf2um/x.dll), in which a specially crafted shader can cause an out of bounds access, which may lead to denial of service or code execution. **CVE ID : CVE-2020-5981**	https://nvidia.custhelp.com/app/answers/detail/a_id/5075	A-NVI-VIRT-191020/122
Allocation of Resources Without Limits or Throttling	02-Oct-20	2.1	NVIDIA Windows GPU Display Driver, all versions, contains a vulnerability in the kernel mode layer (nvlddmkm.sys) scheduler, in which the software does not properly limit the number or frequency of interactions that it has with an actor, such as the number of incoming requests, which may lead	https://nvidia.custhelp.com/app/answers/detail/a_id/5075	A-NVI-VIRT-191020/123

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			to denial of service. **CVE ID : CVE-2020-5982**		
Out-of-bounds Write	02-Oct-20	3.6	NVIDIA Virtual GPU Manager contains a vulnerability in the vGPU plugin and the host driver kernel module, in which the potential exists to write to a memory location that is outside the intended boundary of the frame buffer memory allocated to guest operating systems, which may lead to denial of service or information disclosure. This affects vGPU version 8.x (prior to 8.5), version 10.x (prior to 10.4) and version 11.0. **CVE ID : CVE-2020-5983**	https://nvidia.custhelp.com/app/answers/detail/a_id/5075	A-NVI-VIRT-191020/124
Use After Free	02-Oct-20	4.6	NVIDIA Virtual GPU Manager contains a vulnerability in the vGPU plugin in which it may have the use-after-free vulnerability while freeing some resources, which may lead to denial of service, code execution, and information disclosure. This affects vGPU version 8.x (prior to 8.5), version 10.x (prior to 10.4) and version 11.0. **CVE ID : CVE-2020-5984**	https://nvidia.custhelp.com/app/answers/detail/a_id/5075	A-NVI-VIRT-191020/125
Improper Input Validation	02-Oct-20	3.6	NVIDIA Virtual GPU Manager contains a vulnerability in the vGPU	https://nvidia.custhelp.com/app/answ	A-NVI-VIRT-191020/126

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			plugin, in which an input data length is not validated, which may lead to tampering or denial of service. This affects vGPU version 8.x (prior to 8.5), version 10.x (prior to 10.4) and version 11.0. **CVE ID : CVE-2020-5985**	ers/detail/a_id/5075	
Improper Input Validation	02-Oct-20	2.1	NVIDIA Virtual GPU Manager contains a vulnerability in the vGPU plugin, in which an input data size is not validated, which may lead to tampering or denial of service. This affects vGPU version 8.x (prior to 8.5), version 10.x (prior to 10.4) and version 11.0. **CVE ID : CVE-2020-5986**	https://nvidia.custhelp.com/app/answers/detail/a_id/5075	A-NVI-VIRT-191020/127
Incomplete Cleanup	02-Oct-20	4.6	NVIDIA Virtual GPU Manager contains a vulnerability in the vGPU plugin in which guest-supplied parameters remain writable by the guest after the plugin has validated them, which may lead to the guest being able to pass invalid parameters to plugin handlers, which may lead to denial of service or escalation of privileges. This affects vGPU version 8.x (prior to 8.5), version 10.x (prior to 10.4) and version 11.0.	https://nvidia.custhelp.com/app/answers/detail/a_id/5075	A-NVI-VIRT-191020/128

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2020-5987		
Use After Free	02-Oct-20	3.6	NVIDIA Virtual GPU Manager contains a vulnerability in the vGPU plugin, in which allocated memory can be freed twice, which may lead to information disclosure or denial of service. This affects vGPU version 8.x (prior to 8.5), version 10.x (prior to 10.4) and version 11.0. **CVE ID : CVE-2020-5988**	https://nvidia.custhelp.com/app/answers/detail/a_id/5075	A-NVI-VIRT-191020/129
NULL Pointer Dereference	02-Oct-20	2.1	NVIDIA Virtual GPU Manager contains a vulnerability in the vGPU plugin, in which it can dereference a NULL pointer, which may lead to denial of service. This affects vGPU version 8.x (prior to 8.5), version 10.x (prior to 10.4) and version 11.0. **CVE ID : CVE-2020-5989**	https://nvidia.custhelp.com/app/answers/detail/a_id/5075	A-NVI-VIRT-191020/130
Openmediavault					
openmediavault					
Improper Control of Generation of Code ('Code Injection')	02-Oct-20	9	openmediavault before 4.1.36 and 5.x before 5.5.12 allows authenticated PHP code injection attacks, via the sortfield POST parameter of rpc.php, because json_encode_safe is not used in config/databasebackend.inc. Successful exploitation	https://www.openmediavault.org/?p=2797	A-OPE-OPEN-191020/131

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			allows arbitrary command execution on the underlying operating system as root. **CVE ID : CVE-2020-26124**		
opensc_project					
opensc					
Out-of-bounds Write	06-Oct-20	2.1	The Oberthur smart card software driver in OpenSC before 0.21.0-rc1 has a heap-based buffer overflow in sc_oberthur_read_file. **CVE ID : CVE-2020-26570**	N/A	A-OPE-OPEN-191020/132
Out-of-bounds Write	06-Oct-20	2.1	The gemsafe GPK smart card software driver in OpenSC before 0.21.0-rc1 has a stack-based buffer overflow in sc_pkcs15emu_gemsafeGPK_init. **CVE ID : CVE-2020-26571**	N/A	A-OPE-OPEN-191020/133
Out-of-bounds Write	06-Oct-20	2.1	The TCOS smart card software driver in OpenSC before 0.21.0-rc1 has a stack-based buffer overflow in tcos_decipher. **CVE ID : CVE-2020-26572**	N/A	A-OPE-OPEN-191020/134
PHP					
php					
Inadequate Encryption Strength	02-Oct-20	6.4	In PHP versions 7.2.x below 7.2.34, 7.3.x below 7.3.23 and 7.4.x below 7.4.11, when AES-CCM mode is used with openssl_encrypt() function with 12 bytes IV, only first	N/A	A-PHP-PHP-191020/135

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			7 bytes of the IV is actually used. This can lead to both decreased security and incorrect encryption data. **CVE ID : CVE-2020-7069**		
Reliance on Cookies without Validation and Integrity Checking	02-Oct-20	5	In PHP versions 7.2.x below 7.2.34, 7.3.x below 7.3.23 and 7.4.x below 7.4.11, when PHP is processing incoming HTTP cookie values, the cookie names are url-decoded. This may lead to cookies with prefixes like __Host confused with cookies that decode to such prefix, thus leading to an attacker being able to forge cookie which is supposed to be secure. See also CVE-2020-8184 for more information. **CVE ID : CVE-2020-7070**	N/A	A-PHP-PHP-191020/136
Pluxml					
pluxml					
Improper Control of Generation of Code ('Code Injection')	02-Oct-20	7.5	class.plx.admin.php in PluXml 5.7 allows attackers to execute arbitrary PHP code by modify the configuration file in a linux environment. **CVE ID : CVE-2020-18185**	N/A	A-PLU-PLUX-191020/137
pluxxml					
pluxxml					
N/A	02-Oct-20	6.5	In PluxXml V5.7,the theme edit function /PluXml/core/admin/parametres_edittpl.php allows	N/A	A-PLU-PLUX-191020/138

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			remote attackers to execute arbitrary PHP code by placing this code into a template. **CVE ID : CVE-2020-18184**		
Powerdns					
authoritative					
Information Exposure	02-Oct-20	4	An issue has been found in PowerDNS Authoritative Server before 4.3.1 where an authorized user with the ability to insert crafted records into a zone might be able to leak the content of uninitialized memory. **CVE ID : CVE-2020-17482**	https://doc.powerdns.com/authoritative/security-advisories/powerdns-advisory-2020-05.html	A-POW-AUTH-191020/139
Concurrent Execution using Shared Resource with Improper Synchronization ('Race Condition')	02-Oct-20	5.1	An issue was discovered in PowerDNS Authoritative through 4.3.0 when --enable-experimental-gss-tsig is used. A remote, unauthenticated attacker can trigger a race condition leading to a crash, or possibly arbitrary code execution, by sending crafted queries with a GSS-TSIG signature. **CVE ID : CVE-2020-24696**	N/A	A-POW-AUTH-191020/140
N/A	02-Oct-20	4.3	An issue was discovered in PowerDNS Authoritative through 4.3.0 when --enable-experimental-gss-tsig is used. A remote, unauthenticated attacker can cause a denial of service by sending crafted queries with a GSS-TSIG	https://doc.powerdns.com/authoritative/security-advisories/powerdns-advisory-2020-06.html	A-POW-AUTH-191020/141

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			signature. **CVE ID : CVE-2020-24697**		
Double Free	02-Oct-20	6.8	An issue was discovered in PowerDNS Authoritative through 4.3.0 when --enable-experimental-gss-tsig is used. A remote, unauthenticated attacker might be able to cause a double-free, leading to a crash or possibly arbitrary code execution. by sending crafted queries with a GSS-TSIG signature. **CVE ID : CVE-2020-24698**	https://doc.powerdns.com/authoritative/security-advisories/powerdns-advisory-2020-06.html	A-POW-AUTH-191020/142
pritunl					
pritunl					
Information Exposure	01-Oct-20	5	Pritunl 1.29.2145.25 allows attackers to enumerate valid VPN usernames via a series of /auth/session login attempts. Initially, the server will return error 401. However, if the username is valid, then after 20 login attempts, the server will start responding with error 400. Invalid usernames will receive error 401 indefinitely. **CVE ID : CVE-2020-25200**	N/A	A-PRI-PRIT-191020/143
Qdpm					
qdpm					
Improper Neutralization of Input During	05-Oct-20	3.5	The file upload functionality in qdPM 9.1 doesn't check the file	N/A	A-QDP-QDPM-191020/144

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Web Page Generation ('Cross-site Scripting')			description, which allows remote authenticated attackers to inject web script or HTML via the attachments info parameter, aka XSS. This can occur during creation of a ticket, project, or task. **CVE ID : CVE-2020-26166**		
Qemu					
qemu					
NULL Pointer Dereference	02-Oct-20	2.1	fdctrl_write_data in hw/block/fdc.c in QEMU 5.0.0 has a NULL pointer dereference via a NULL block pointer for the current drive. **CVE ID : CVE-2020-25741**	http://www.openwall.com/lists/oss-security/2020/09/29/1, https://security.netapp.com/advisory/ntap-20201009-0005/	A-QEM-QEMU-191020/145
NULL Pointer Dereference	06-Oct-20	2.1	pci_change_irq_level in hw/pci/pci.c in QEMU before 5.1.1 has a NULL pointer dereference because pci_get_bus() might not return a valid pointer. **CVE ID : CVE-2020-25742**	http://www.openwall.com/lists/oss-security/2020/09/29/1	A-QEM-QEMU-191020/146
NULL Pointer Dereference	06-Oct-20	2.1	hw/ide/pci.c in QEMU before 5.1.1 can trigger a NULL pointer dereference because it lacks a pointer check before an ide_cancel_dma_sync call. **CVE ID : CVE-2020-25743**	http://www.openwall.com/lists/oss-security/2020/09/29/1	A-QEM-QEMU-191020/147
Redhat					

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
openshift_application_runtimes					
Uncontrolled Resource Consumption	06-Oct-20	5	A memory leak flaw was found in WildFly OpenSSL in versions prior to 1.1.3.Final, where it removes an HTTP session. It may allow the attacker to cause OOM leading to a denial of service. The highest threat from this vulnerability is to system availability. **CVE ID : CVE-2020-25644**	N/A	A-RED-OPEN-191020/148
jboss_data_grid					
Uncontrolled Resource Consumption	06-Oct-20	5	A memory leak flaw was found in WildFly OpenSSL in versions prior to 1.1.3.Final, where it removes an HTTP session. It may allow the attacker to cause OOM leading to a denial of service. The highest threat from this vulnerability is to system availability. **CVE ID : CVE-2020-25644**	N/A	A-RED-JBOS-191020/149
jboss_fuse					
Uncontrolled Resource Consumption	06-Oct-20	5	A memory leak flaw was found in WildFly OpenSSL in versions prior to 1.1.3.Final, where it removes an HTTP session. It may allow the attacker to cause OOM leading to a denial of service. The highest threat from this vulnerability is to system availability.	N/A	A-RED-JBOS-191020/150

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2020-25644		
openstack_platform					
NULL Pointer Dereference	06-Oct-20	2.1	hw/ide/pci.c in QEMU before 5.1.1 can trigger a NULL pointer dereference because it lacks a pointer check before an ide_cancel_dma_sync call. **CVE ID : CVE-2020-25743**	http://www.openwall.com/lists/oss-security/2020/09/29/1	A-RED-OPEN-191020/151
wildfly_openssl					
Uncontrolled Resource Consumption	06-Oct-20	5	A memory leak flaw was found in WildFly OpenSSL in versions prior to 1.1.3.Final, where it removes an HTTP session. It may allow the attacker to cause OOM leading to a denial of service. The highest threat from this vulnerability is to system availability. **CVE ID : CVE-2020-25644**	N/A	A-RED-WILD-191020/152
data_grid					
Uncontrolled Resource Consumption	06-Oct-20	5	A memory leak flaw was found in WildFly OpenSSL in versions prior to 1.1.3.Final, where it removes an HTTP session. It may allow the attacker to cause OOM leading to a denial of service. The highest threat from this vulnerability is to system availability. **CVE ID : CVE-2020-25644**	N/A	A-RED-DATA-191020/153
jboss_enterprise_application_platform					
Uncontrolled Resource	06-Oct-20	5	A memory leak flaw was found in WildFly OpenSSL	N/A	A-RED-JBOS-

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Consumption			in versions prior to 1.1.3.Final, where it removes an HTTP session. It may allow the attacker to cause OOM leading to a denial of service. The highest threat from this vulnerability is to system availability. **CVE ID : CVE-2020-25644**		191020/154
single_sign-on					
Uncontrolled Resource Consumption	06-Oct-20	5	A memory leak flaw was found in WildFly OpenSSL in versions prior to 1.1.3.Final, where it removes an HTTP session. It may allow the attacker to cause OOM leading to a denial of service. The highest threat from this vulnerability is to system availability. **CVE ID : CVE-2020-25644**	N/A	A-RED-SING-191020/155
ansible					
Improper Cross-boundary Removal of Sensitive Data	05-Oct-20	2.1	A flaw was found in Ansible Base when using the aws_ssm connection plugin as garbage collector is not happening after playbook run is completed. Files would remain in the bucket exposing the data. This issue affects directly data confidentiality. **CVE ID : CVE-2020-25635**	https://bugzilla.redhat.com/show_bug.cgi?id=CVE-2020-25635	A-RED-ANSI-191020/156
Files or Directories Accessible to External	05-Oct-20	3.6	A flaw was found in Ansible Base when using the aws_ssm connection plugin as there is no	https://bugzilla.redhat.com/show_bug.cgi?id=CVE-	A-RED-ANSI-191020/157

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Parties			namespace separation for file transfers. Files are written directly to the root bucket, making possible to have collisions when running multiple ansible processes. This issue affects mainly the service availability. **CVE ID : CVE-2020-25636**	2020-25636	
libvirt					
Double Free	06-Oct-20	7.2	A double free memory issue was found to occur in the libvirt API, in versions before 6.8.0, responsible for requesting information about network interfaces of a running QEMU domain. This flaw affects the polkit access control driver. Specifically, clients connecting to the read-write socket with limited ACL permissions could use this flaw to crash the libvirt daemon, resulting in a denial of service, or potentially escalate their privileges on the system. The highest threat from this vulnerability is to data confidentiality and integrity as well as system availability. **CVE ID : CVE-2020-25637**	N/A	A-RED-LIBV-191020/158
requarks					
wiki.js					
Improper Limitation of a	05-Oct-20	5	In Wiki.js before version 2.5.151, directory	https://github.com/Requa	A-REQ-WIKI-191020/159

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Pathname to a Restricted Directory ('Path Traversal')			traversal outside of Wiki.js context is possible when a storage module with local asset cache fetching is enabled. A malicious user can potentially read any file on the file system by crafting a special URL that allows for directory traversal. This is only possible when a storage module implementing local asset cache (e.g Local File System or Git) is enabled and that no web application firewall solution (e.g. cloudflare) strips potentially malicious URLs. Commit 084dcd69d1591586ee4752101e675d5f0ac6dcdc fixes this vulnerability by sanitizing the path before it is passed on to the storage module. The sanitization step removes any directory traversal (e.g. `..` and `.`) sequences as well as invalid filesystem characters from the path. As a workaround, disable any storage module with local asset caching capabilities such as Local File System and Git. **CVE ID : CVE-2020-15236**	rks/wiki/security/advisories/GHSA-whpv-5xg2-w527	
safetydance_project					
safetydance					
Improper	02-Oct-20	7.5	All versions of package	N/A	A-SAF-SAFE-

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Input Validation			safetydance are vulnerable to Prototype Pollution via the set function. **CVE ID : CVE-2020-7737**		191020/160
secudos					
domos					
Improper Neutralization of Special Elements used in an OS Command ('OS Command Injection')	02-Oct-20	8.5	conf_datetime in Secudos DOMOS 5.8 allows remote attackers to execute arbitrary commands as root via shell metacharacters in the zone field (obtained from the web interface). **CVE ID : CVE-2020-14293**	N/A	A-SEC-DOMO-191020/161
qiata_fta					
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	02-Oct-20	4.3	An issue was discovered in Secudos Qiata FTA 1.70.19. The comment feature allows persistent XSS that is executed when reading transfer comments or the global notice board. **CVE ID : CVE-2020-14294**	N/A	A-SEC-QIAT-191020/162
shiba_project					
shiba					
N/A	02-Oct-20	6.5	All versions of package shiba are vulnerable to Arbitrary Code Execution due to the default usage of the function load() of the package js-yaml instead of its secure replacement , safeLoad(). **CVE ID : CVE-2020-7738**	https://snyk.io/vuln/SNYK-JS-SHIBA-596466	A-SHI-SHIB-191020/163
simpl-schema_project					

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
simpl-schema					
N/A	07-Oct-20	5	This affects the package simpl-schema before 1.10.2. **CVE ID : CVE-2020-7742**	N/A	A-SIM-SIMP-191020/164
smallpdf					
json-pointer					
Improper Input Validation	05-Oct-20	6.5	This affects the package json-pointer before 0.6.1. Multiple reference of object using slash is supported. **CVE ID : CVE-2020-7709**	N/A	A-SMA-JSON-191020/165
socket.io-file_project					
socket.io-file					
Improper Input Validation	06-Oct-20	6.8	** UNSUPPORTED WHEN ASSIGNED ** The socket.io-file package through 2.0.31 for Node.js relies on client-side validation of file types, which allows remote attackers to execute arbitrary code by uploading an executable file via a modified JSON name field. NOTE: This vulnerability only affects products that are no longer supported by the maintainer. **CVE ID : CVE-2020-24807**	N/A	A-SOC-SOCK-191020/166
Sysaid					
sysaid_on-premises					
Improper Neutralization of Input During	02-Oct-20	4.3	SysAid 20.1.11b26 allows reflected XSS via the ForgotPassword.jsp	N/A	A-SYS-SYSA-191020/167

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Web Page Generation ('Cross-site Scripting')			accountid parameter. **CVE ID : CVE-2020-13168**		
sysaidsy_on-premises					
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	02-Oct-20	4.3	SysAid 20.1.11b26 allows reflected XSS via the ForgotPassword.jsp accountid parameter. **CVE ID : CVE-2020-13168**	N/A	A-SYS-SYSA-191020/168
Trendmicro					
antivirus					
Improper Privilege Management	02-Oct-20	7.2	Trend Micro Antivirus for Mac 2020 (Consumer) is vulnerable to a symbolic link privilege escalation attack where an attacker could exploit a critical file on the system to escalate their privileges. An attacker must first obtain the ability to execute low-privileged code on the target system in order to exploit this vulnerability. **CVE ID : CVE-2020-25776**	N/A	A-TRE-ANTI-191020/169
Trustwave					
modsecurity					
Loop with Unreachable Exit Condition ('Infinite Loop')	06-Oct-20	5	** DISPUTED ** Trustwave ModSecurity 3.x through 3.0.4 allows denial of service via a special request. NOTE: The discoverer reports "Trustwave has signaled they are disputing our	https://www.debian.org/security/2020/dsa-4765	A-TRU-MODS-191020/170

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			claims." The CVE suggests that there is a security issue with how ModSecurity handles regular expressions that can result in a Denial of Service condition. The vendor does not consider this as a security issue because1) there is no default configuration issue here. An attacker would need to know that a rule using a potentially problematic regular expression was in place, 2) the attacker would need to know the basic nature of the regular expression itself to exploit any resource issues. It's well known that regular expression usage can be taxing on system resources regardless of the use case. It is up to the administrator to decide on when it is appropriate to trade resources for potential security benefit. **CVE ID : CVE-2020-15598**		
Unisys					
stealth					
Use of Hard-coded Credentials	01-Oct-20	2.1	Unisys Stealth(core) before 4.0.134 stores passwords in a recoverable format. Therefore, a search of Enterprise Manager can potentially reveal	https://public.support.unisys.com/common/public/vulnerability/NVD_Detail_Rpt.aspx?ID=	A-UNI-STEA-191020/171

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			credentials. **CVE ID : CVE-2020-24620**	56	
vapor_project					
vapor					
Improper Limitation of a Pathname to a Restricted Directory ('Path Traversal')	02-Oct-20	4	Vapor is a web framework for Swift. In Vapor before version 4.29.4, Attackers can access data at arbitrary filesystem paths on the same host as an application. Only applications using FileMiddleware are affected. This is fixed in version 4.29.4. **CVE ID : CVE-2020-15230**	https://github.com/vapor/vapor/security/advisories/GHSA-vcvg-xgr8-p5gq	A-VAP-VAPO-191020/172
Websitebaker					
websitebaker					
Improper Neutralization of Special Elements used in an SQL Command ('SQL Injection')	01-Oct-20	7.5	WebsiteBaker 2.12.2 allows SQL Injection via parameter 'display_name' in /websitebaker/admin/preferences/save.php. Exploiting this issue could allow an attacker to compromise the application, access or modify data, or exploit latent vulnerabilities in the underlying database. **CVE ID : CVE-2020-25990**	N/A	A-WEB-WEBS-191020/173
whatsapp					
whatsapp					
Information Exposure	06-Oct-20	5	A user running a quick search on a highly forwarded message on	https://www.whatsapp.com/security	A-WHA-WHAT-191020/174

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			WhatsApp for Android from v2.20.108 to v2.20.140 or WhatsApp Business for Android from v2.20.35 to v2.20.49 could have been sent to the Google service over plain HTTP. **CVE ID : CVE-2020-1902**	/advisories/2020/	
Improper Limitation of a Pathname to a Restricted Directory ('Path Traversal')	06-Oct-20	5.8	A path validation issue in WhatsApp for iOS prior to v2.20.61 and WhatsApp Business for iOS prior to v2.20.61 could have allowed for directory traversal overwriting files when sending specially crafted docx, xlx, and pptx files as attachments to messages. **CVE ID : CVE-2020-1904**	https://www.whatsapp.com/security/advisories/2020/	A-WHA-WHAT-191020/175
Use of Insufficiently Random Values	06-Oct-20	4.3	Media ContentProvider URIs used for opening attachments in other apps were generated sequentially prior to WhatsApp for Android v2.20.185, which could have allowed a malicious third party app chosen to open the file to guess the URIs for previously opened attachments until the opener app is terminated. **CVE ID : CVE-2020-1905**	https://www.whatsapp.com/security/advisories/2020/	A-WHA-WHAT-191020/176
Out-of-bounds Write	06-Oct-20	4.6	A buffer overflow in WhatsApp for Android prior to v2.20.130 and	https://www.whatsapp.com/security	A-WHA-WHAT-191020/177

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			WhatsApp Business for Android prior to v2.20.46 could have allowed an out-of-bounds write when processing malformed local videos with E-AC-3 audio streams. **CVE ID : CVE-2020-1906**	/advisories/2020/	
whatsapp_business					
Information Exposure	06-Oct-20	5	A user running a quick search on a highly forwarded message on WhatsApp for Android from v2.20.108 to v2.20.140 or WhatsApp Business for Android from v2.20.35 to v2.20.49 could have been sent to the Google service over plain HTTP. **CVE ID : CVE-2020-1902**	https://www.whatsapp.com/security/advisories/2020/	A-WHA-WHAT-191020/178
Improper Limitation of a Pathname to a Restricted Directory ('Path Traversal')	06-Oct-20	5.8	A path validation issue in WhatsApp for iOS prior to v2.20.61 and WhatsApp Business for iOS prior to v2.20.61 could have allowed for directory traversal overwriting files when sending specially crafted docx, xlx, and pptx files as attachments to messages. **CVE ID : CVE-2020-1904**	https://www.whatsapp.com/security/advisories/2020/	A-WHA-WHAT-191020/179
Out-of-bounds Write	06-Oct-20	4.6	A buffer overflow in WhatsApp for Android prior to v2.20.130 and WhatsApp Business for Android prior to v2.20.46 could have allowed an out-	https://www.whatsapp.com/security/advisories/2020/	A-WHA-WHAT-191020/180

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			of-bounds write when processing malformed local videos with E-AC-3 audio streams. **CVE ID : CVE-2020-1906**		
Wireshark					
wireshark					
Improper Validation of Integrity Check Value	06-Oct-20	5	In Wireshark 3.2.0 to 3.2.6, 3.0.0 to 3.0.13, and 2.6.0 to 2.6.20, the TCP dissector could crash. This was addressed in epan/dissectors/packet-tcp.c by changing the handling of the invalid 0xFFFF checksum. **CVE ID : CVE-2020-25862**	N/A	A-WIR-WIRE-191020/181
N/A	06-Oct-20	5	In Wireshark 3.2.0 to 3.2.6, 3.0.0 to 3.0.13, and 2.6.0 to 2.6.20, the MIME Multipart dissector could crash. This was addressed in epan/dissectors/packet-multipart.c by correcting the deallocation of invalid MIME parts. **CVE ID : CVE-2020-25863**	N/A	A-WIR-WIRE-191020/182
NULL Pointer Dereference	06-Oct-20	5	In Wireshark 3.2.0 to 3.2.6 and 3.0.0 to 3.0.13, the BLIP protocol dissector has a NULL pointer dereference because a buffer was sized for compressed (not uncompressed) messages. This was addressed in epan/dissectors/packet-blip.c by allowing reasonable compression	N/A	A-WIR-WIRE-191020/183

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			ratios and rejecting ZIP bombs. **CVE ID : CVE-2020-25866**		
wpo365					
wordpress_\+_azure_ad_\/_microsoft_office_365					
N/A	02-Oct-20	5	The wpo365-login plugin before v11.7 for WordPress allows use of a symmetric algorithm to decrypt a JWT token. This leads to authentication bypass. **CVE ID : CVE-2020-26511**	N/A	A-WPO-WORD-191020/184
Zohocorp					
manageengine_desktop_central					
N/A	02-Oct-20	6.8	A design issue was discovered in GetInternetRequestHandle, InternetSendRequestEx and InternetSendRequestByBitrate in the client side of Zoho ManageEngine Desktop Central 10.0.552.W. By exploiting this issue, an attacker-controlled server can force the client to skip TLS certificate validation, leading to a man-in-the-middle attack against HTTPS and unauthenticated remote code execution. **CVE ID : CVE-2020-15589**	https://www.manageengine.com/products/desktop-central/untrusted-agent-server-communication.html	A-ZOH-MANA-191020/185
Integer Overflow or Wraparound	02-Oct-20	9	An issue was discovered in the client side of Zoho ManageEngine Desktop	https://www.manageengine.com/pr	A-ZOH-MANA-191020/186

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Central 10.0.0.SP-534. An attacker-controlled server can trigger an integer overflow in InternetSendRequestEx and InternetSendRequestByBitrate that leads to a heap-based buffer overflow and Remote Code Execution with SYSTEM privileges. **CVE ID : CVE-2020-24397**	oducts/desktop-central/integer-overflow-vulnerability.html	
manageengine_applications_manager					
Improper Neutralization of Special Elements used in an SQL Command ('SQL Injection')	01-Oct-20	7.5	In Zoho ManageEngine Application Manager 14.7 Build 14730 (before 14684, and between 14689 and 14750), the AlarmEscalation module is vulnerable to unauthenticated SQL Injection attack. **CVE ID : CVE-2020-15533**	https://www.manageengine.com/products/applications_manager/issues.html#v14750, https://www.manageengine.com/products/applications_manager/security-updates/security-updates-cve-2020-15533.html	A-ZOH-MANA-191020/187
Improper Neutralization of Special Elements used in an SQL Command ('SQL Injection')	06-Oct-20	6.5	Zoho ManageEngine Applications Manager version 14740 and prior allows an authenticated SQL Injection via a crafted jsp request in the SAP module.	https://www.manageengine.com/products/applications_manager/issues.html#v14750, https://ww	A-ZOH-MANA-191020/188

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2020-15927	w.manageengine.com/products/applications_manager/security-updates/security-updates-cve-2020-15927.html	
Improper Neutralization of Special Elements used in an SQL Command ('SQL Injection')	06-Oct-20	6.5	Zoho ManageEngine Applications Manager version 14740 and prior allows an authenticated SQL Injection via a crafted jsp request in the RCA module. **CVE ID : CVE-2020-16267**	https://www.manageengine.com/products/applications_manager/issues.html#v14750, https://www.manageengine.com/products/applications_manager/security-updates/security-updates-cve-2020-16267.html	A-ZOH-MANA-191020/189
Operating System					
Apple					
mac_os					
Improper Control of Generation of Code ('Code Injection')	02-Oct-20	5	An issue was discovered in Foxit Reader and PhantomPDF before 4.1 on macOS. Because the Hardened Runtime protection mechanism is not applied to code	N/A	O-APP-MAC_-191020/190

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			signing, code injection (or an information leak) can occur. **CVE ID : CVE-2020-26540**		
Debian					
debian_linux					
Loop with Unreachable Exit Condition ('Infinite Loop')	06-Oct-20	5	** DISPUTED ** Trustwave ModSecurity 3.x through 3.0.4 allows denial of service via a special request. NOTE: The discoverer reports "Trustwave has signaled they are disputing our claims." The CVE suggests that there is a security issue with how ModSecurity handles regular expressions that can result in a Denial of Service condition. The vendor does not consider this as a security issue because1) there is no default configuration issue here. An attacker would need to know that a rule using a potentially problematic regular expression was in place, 2) the attacker would need to know the basic nature of the regular expression itself to exploit any resource issues. It's well known that regular expression usage can be taxing on system resources regardless of the use case. It is up to the	https://www.debian.org/security/2020/dsa-4765	O-DEB-DEBI-191020/191

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			administrator to decide on when it is appropriate to trade resources for potential security benefit. **CVE ID : CVE-2020-15598**		
Reliance on Cookies without Validation and Integrity Checking	02-Oct-20	5	In PHP versions 7.2.x below 7.2.34, 7.3.x below 7.3.23 and 7.4.x below 7.4.11, when PHP is processing incoming HTTP cookie values, the cookie names are url-decoded. This may lead to cookies with prefixes like __Host confused with cookies that decode to such prefix, thus leading to an attacker being able to forge cookie which is supposed to be secure. See also CVE-2020-8184 for more information. **CVE ID : CVE-2020-7070**	N/A	O-DEB-DEBI-191020/192
Dell					
xps_13_9370_firmware					
Improper Handling of Exceptional Conditions	01-Oct-20	4.9	Dell XPS 13 9370 BIOS versions prior to 1.13.1 contains an Improper Exception Handling vulnerability. A local attacker with physical access could exploit this vulnerability to prevent the system from booting until the exploited boot device is removed. **CVE ID : CVE-2020-5387**	https://www.dell.com/support/article/SLN322626	O-DEL-XPS_-191020/193
elecom					

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
wrc-2533gst2_firmware					
N/A	06-Oct-20	8.3	ELECOM LAN routers (WRC-2533GST2 firmware versions prior to v1.14, WRC-1900GST2 firmware versions prior to v1.14, WRC-1750GST2 firmware versions prior to v1.14, and WRC-1167GST2 firmware versions prior to v1.10) allow an attacker on the same network segment to execute arbitrary OS commands with a root privilege via unspecified vectors. **CVE ID : CVE-2020-5634**	N/A	O-ELE-WRC--191020/194
wrc-1900gst2_firmware					
N/A	06-Oct-20	8.3	ELECOM LAN routers (WRC-2533GST2 firmware versions prior to v1.14, WRC-1900GST2 firmware versions prior to v1.14, WRC-1750GST2 firmware versions prior to v1.14, and WRC-1167GST2 firmware versions prior to v1.10) allow an attacker on the same network segment to execute arbitrary OS commands with a root privilege via unspecified vectors. **CVE ID : CVE-2020-5634**	N/A	O-ELE-WRC--191020/195
wrc-1750gst2_firmware					
N/A	06-Oct-20	8.3	ELECOM LAN routers (WRC-2533GST2 firmware versions prior to v1.14, WRC-1900GST2 firmware	N/A	O-ELE-WRC--191020/196

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			versions prior to v1.14, WRC-1750GST2 firmware versions prior to v1.14, and WRC-1167GST2 firmware versions prior to v1.10) allow an attacker on the same network segment to execute arbitrary OS commands with a root privilege via unspecified vectors. **CVE ID : CVE-2020-5634**		
wrc-1167gst2_firmware					
N/A	06-Oct-20	8.3	ELECOM LAN routers (WRC-2533GST2 firmware versions prior to v1.14, WRC-1900GST2 firmware versions prior to v1.14, WRC-1750GST2 firmware versions prior to v1.14, and WRC-1167GST2 firmware versions prior to v1.10) allow an attacker on the same network segment to execute arbitrary OS commands with a root privilege via unspecified vectors. **CVE ID : CVE-2020-5634**	N/A	O-ELE-WRC--191020/197
Fedoraproject					
fedora					
Inadequate Encryption Strength	02-Oct-20	6.4	In PHP versions 7.2.x below 7.2.34, 7.3.x below 7.3.23 and 7.4.x below 7.4.11, when AES-CCM mode is used with openssl_encrypt() function with 12 bytes IV, only first 7 bytes of the IV is actually	N/A	O-FED-FEDO-191020/198

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			used. This can lead to both decreased security and incorrect encryption data. **CVE ID : CVE-2020-7069**		
Reliance on Cookies without Validation and Integrity Checking	02-Oct-20	5	In PHP versions 7.2.x below 7.2.34, 7.3.x below 7.3.23 and 7.4.x below 7.4.11, when PHP is processing incoming HTTP cookie values, the cookie names are url-decoded. This may lead to cookies with prefixes like __Host confused with cookies that decode to such prefix, thus leading to an attacker being able to forge cookie which is supposed to be secure. See also CVE-2020-8184 for more information. **CVE ID : CVE-2020-7070**	N/A	O-FED-FEDO-191020/199
Google					
android					
Improper Input Validation	06-Oct-20	5	An issue was discovered on LG mobile devices with Android OS 9.0 and 10 software. The Wi-Fi subsystem has incorrect input validation, leading to a crash. The LG ID is LVE-SMP-200022 (October 2020). **CVE ID : CVE-2020-26597**	N/A	O-GOO-ANDR-191020/200
Missing Authorization	06-Oct-20	5	An issue was discovered on LG mobile devices with Android OS 8.0, 8.1, and 9.0 software. The Network Management component	N/A	O-GOO-ANDR-191020/201

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			could allow an unauthorized actor to kill a TCP connection. The LG ID is LVE-SMP-200023 (October 2020). **CVE ID : CVE-2020-26598**		
Improper Authentication	06-Oct-20	5	An issue was discovered on Samsung mobile devices with Q(10.0) software. The DynamicLockscreen Terms and Conditions can be accepted without authentication. The Samsung ID is SVE-2020-17079 (October 2020). **CVE ID : CVE-2020-26599**	N/A	O-GOO-ANDR-191020/202
Information Exposure	06-Oct-20	5	An issue was discovered on Samsung mobile devices with Q(10.0) software. Auto Hotspot allows attackers to obtain sensitive information. The Samsung ID is SVE-2020-17288 (October 2020). **CVE ID : CVE-2020-26600**	N/A	O-GOO-ANDR-191020/203
Improper Privilege Management	06-Oct-20	5	An issue was discovered in DirEncryptService on Samsung mobile devices with O(8.x), P(9.0), and Q(10.0) software. PendingIntent with an empty intent is mishandled, allowing an attacker to perform a privileged action via a modified intent. The Samsung ID is SVE-2020-18034 (October 2020).	N/A	O-GOO-ANDR-191020/204

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2020-26601		
Exposure of Resource to Wrong Sphere	06-Oct-20	5	An issue was discovered in EthernetNetwork on Samsung mobile devices with O(8.1), P(9.0), Q(10.0), and R(11.0) software. PendingIntent allows sdcard access by an unprivileged process. The Samsung ID is SVE-2020-18392 (October 2020). **CVE ID : CVE-2020-26602**	N/A	O-GOO-ANDR-191020/205
Improper Limitation of a Pathname to a Restricted Directory ('Path Traversal')	06-Oct-20	5	An issue was discovered on Samsung mobile devices with O(8.x), P(9.0), and Q(10.0) software. Sticker Center allows directory traversal for an unprivileged process to read arbitrary files. The Samsung ID is SVE-2020-18433 (October 2020). **CVE ID : CVE-2020-26603**	N/A	O-GOO-ANDR-191020/206
Improper Privilege Management	06-Oct-20	5	An issue was discovered in SystemUI on Samsung mobile devices with O(8.x), P(9.0), Q(10.0), and R(11.0) software. PendingIntent allows an unprivileged process to access contact numbers. The Samsung ID is SVE-2020-18467 (October 2020). **CVE ID : CVE-2020-26604**	N/A	O-GOO-ANDR-191020/207
Information Exposure Through Log Files	06-Oct-20	5	An issue was discovered on Samsung mobile devices with Q(10.0) and R(11.0) (Exynos chipsets)	N/A	O-GOO-ANDR-191020/208

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			software. They allow attackers to obtain sensitive information by reading a log. The Samsung ID is SVE-2020-18596 (October 2020). **CVE ID : CVE-2020-26605**		
Information Exposure	06-Oct-20	5	An issue was discovered on Samsung mobile devices with O(8.x), P(9.0), Q(10.0), and R(11.0) software. An attacker can access certain Secure Folder content via a debugging command. The Samsung ID is SVE-2020-18673 (October 2020). **CVE ID : CVE-2020-26606**	N/A	O-GOO-ANDR-191020/209
Improper Privilege Management	06-Oct-20	7.5	An issue was discovered in TimaService on Samsung mobile devices with O(8.x), P(9.0), and Q(10.0) software. PendingIntent with an empty intent is mishandled, allowing an attacker to perform a privileged action via a modified intent. The Samsung ID is SVE-2020-18418 (October 2020). **CVE ID : CVE-2020-26607**	N/A	O-GOO-ANDR-191020/210
hpe					
kvm_ip_console_switch_g2_firmware					
Improper Neutralization of Input During Web Page Generation ('Cross-site	02-Oct-20	3.5	A remote stored xss vulnerability was discovered in HPE KVM IP Console Switches version(s): G2 4x1Ex32	N/A	O-HPE-KVM_-191020/211

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Scripting')			Prior to 2.8.3. **CVE ID : CVE-2020-24627**		
Improper Control of Generation of Code ('Code Injection')	02-Oct-20	6.5	A remote code injection vulnerability was discovered in HPE KVM IP Console Switches version(s): G2 4x1Ex32 Prior to 2.8.3. **CVE ID : CVE-2020-24628**	N/A	O-HPE-KVM_-191020/212
Linux					
linux_kernel					
Loop with Unreachable Exit Condition ('Infinite Loop')	06-Oct-20	4.9	A flaw was found in the Linux kernel's implementation of biovecs in versions before 5.9-rc7. A zero-length biovec request issued by the block subsystem could cause the kernel to enter an infinite loop, causing a denial of service. This flaw allows a local attacker with basic privileges to issue requests to a block device, resulting in a denial of service. The highest threat from this vulnerability is to system availability. **CVE ID : CVE-2020-25641**	N/A	O-LIN-LINU-191020/213
N/A	02-Oct-20	6.9	The Linux kernel through 5.8.13 does not properly enforce the Secure Boot Forbidden Signature Database (aka dbx) protection mechanism. This affects certs/blacklist.c and	N/A	O-LIN-LINU-191020/214

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			certs/system_keyring.c. **CVE ID : CVE-2020-26541**		
msi					
ambientlink_mslo64_firmware					
Out-of-bounds Write	02-Oct-20	7.2	The MSI AmbientLink MsIo64 driver 1.0.0.8 has a Buffer Overflow (0x80102040, 0x80102044, 0x80102050,and 0x80102054). **CVE ID : CVE-2020-17382**	N/A	O-MSI-AMBI-191020/215
Redhat					
enterprise_linux					
Double Free	06-Oct-20	7.2	A double free memory issue was found to occur in the libvirt API, in versions before 6.8.0, responsible for requesting information about network interfaces of a running QEMU domain. This flaw affects the polkit access control driver. Specifically, clients connecting to the read-write socket with limited ACL permissions could use this flaw to crash the libvirt daemon, resulting in a denial of service, or potentially escalate their privileges on the system. The highest threat from this vulnerability is to data confidentiality and integrity as well as system availability. **CVE ID : CVE-2020-25637**	N/A	O-RED-ENTE-191020/216

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Loop with Unreachable Exit Condition ('Infinite Loop')	06-Oct-20	4.9	A flaw was found in the Linux kernel's implementation of biovecs in versions before 5.9-rc7. A zero-length biovec request issued by the block subsystem could cause the kernel to enter an infinite loop, causing a denial of service. This flaw allows a local attacker with basic privileges to issue requests to a block device, resulting in a denial of service. The highest threat from this vulnerability is to system availability. **CVE ID : CVE-2020-25641**	N/A	O-RED-ENTE-191020/217
NULL Pointer Dereference	06-Oct-20	2.1	hw/ide/pci.c in QEMU before 5.1.1 can trigger a NULL pointer dereference because it lacks a pointer check before an ide_cancel_dma_sync call. **CVE ID : CVE-2020-25743**	http://www.openwall.com/lists/oss-security/2020/09/29/1	O-RED-ENTE-191020/218
Sierrawireless					
aleos					
Improper Input Validation	06-Oct-20	7.2	Lack of input sanitization in UpdateRebootMgr service of ALEOS 4.11 and later allow an escalation to root from a low-privilege process. **CVE ID : CVE-2020-8781**	https://source.sierrawireless.com/resources/security-bulletins/sierra-wireless-technical-bulletin---swi-psa-2020-005/	O-SIE-ALEO-191020/219

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
N/A	06-Oct-20	7.5	Unauthenticated RPC server on ALEOS before 4.4.9, 4.9.5, and 4.14.0 allows remote code execution. **CVE ID : CVE-2020-8782**	https://source.sierrawireless.com/resources/security-bulletins/sierra-wireless-technical-bulletin---swi-psa-2020-005/	O-SIE-ALEO-191020/220
teltonika-networks					
trb245_firmware					
Server-Side Request Forgery (SSRF)	01-Oct-20	4	Server-Side Request Forgery in Teltonika firmware TRB2_R_00.02.04.3 allows a low privileged user to cause the application to perform HTTP GET requests to arbitrary URLs. **CVE ID : CVE-2020-5784**	N/A	O-TEL-TRB2-191020/221
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	01-Oct-20	4.3	Insufficient output sanitization in Teltonika firmware TRB2_R_00.02.04.3 allows an unauthenticated attacker to conduct reflected cross-site scripting via a crafted 'action' or 'pkg_name' parameter. **CVE ID : CVE-2020-5785**	N/A	O-TEL-TRB2-191020/222
Cross-Site Request Forgery (CSRF)	01-Oct-20	6.8	Cross-site request forgery in Teltonika firmware TRB2_R_00.02.04.3 allows a remote attacker to perform sensitive application actions by	N/A	O-TEL-TRB2-191020/223

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			tricking legitimate users into clicking a crafted link. **CVE ID : CVE-2020-5786**		
Improper Limitation of a Pathname to a Restricted Directory ('Path Traversal')	01-Oct-20	8.5	Relative Path Traversal in Teltonika firmware TRB2_R_00.02.04.3 allows a remote, authenticated attacker to delete arbitrary files on disk via the admin/services/packages/remove action. **CVE ID : CVE-2020-5787**	N/A	O-TEL-TRB2-191020/224
Improper Limitation of a Pathname to a Restricted Directory ('Path Traversal')	01-Oct-20	8.5	Relative Path Traversal in Teltonika firmware TRB2_R_00.02.04.3 allows a remote, authenticated attacker to delete arbitrary files on disk via the admin/system/admin/certificates/delete action. **CVE ID : CVE-2020-5788**	N/A	O-TEL-TRB2-191020/225
Improper Limitation of a Pathname to a Restricted Directory ('Path Traversal')	01-Oct-20	4	Relative Path Traversal in Teltonika firmware TRB2_R_00.02.04.3 allows a remote, authenticated attacker to read the contents of arbitrary files on disk. **CVE ID : CVE-2020-5789**	N/A	O-TEL-TRB2-191020/226
wavlink					
wn530h4_firmware					
Cross-Site Request Forgery (CSRF)	02-Oct-20	7.8	CSRF vulnerabilities in the /cgi-bin/ directory of the WAVLINK WN530H4 M30H4.V5030.190403 allow an attacker to remotely access router endpoints, because these	N/A	O-WAV-WN53-191020/227

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			endpoints do not contain CSRF tokens. If a user is authenticated in the router portal, then this attack will work. **CVE ID : CVE-2020-12123**		
Improper Neutralization of Special Elements used in an OS Command ('OS Command Injection')	02-Oct-20	10	A remote command-line injection vulnerability in the /cgi-bin/live_api.cgi endpoint of the WAVLINK WN530H4 M30H4.V5030.190403 allows an attacker to execute arbitrary Linux commands as root without authentication. **CVE ID : CVE-2020-12124**	N/A	O-WAV-WN53-191020/228
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	02-Oct-20	10	A remote buffer overflow vulnerability in the /cgi-bin/makeRequest.cgi endpoint of the WAVLINK WN530H4 M30H4.V5030.190403 allows an attacker to execute arbitrary machine instructions as root without authentication. **CVE ID : CVE-2020-12125**	N/A	O-WAV-WN53-191020/229
Improper Authentication	02-Oct-20	7.5	Multiple authentication bypass vulnerabilities in the /cgi-bin/ endpoint of the WAVLINK WN530H4 M30H4.V5030.190403 allow an attacker to leak router settings, change configuration variables, and cause denial of service via an unauthenticated endpoint.	N/A	O-WAV-WN53-191020/230

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2020-12126		
Information Exposure	02-Oct-20	5	An information disclosure vulnerability in the /cgi-bin/ExportAllSettings.sh endpoint of the WAVLINK WN530H4 M30H4.V5030.190403 allows an attacker to leak router settings, including cleartext login details, DNS settings, and other sensitive information without authentication. **CVE ID : CVE-2020-12127**	N/A	O-WAV-WN53-191020/231
Hardware					
Dell					
xps_13_9370					
Improper Handling of Exceptional Conditions	01-Oct-20	4.9	Dell XPS 13 9370 BIOS versions prior to 1.13.1 contains an Improper Exception Handling vulnerability. A local attacker with physical access could exploit this vulnerability to prevent the system from booting until the exploited boot device is removed. **CVE ID : CVE-2020-5387**	https://www.dell.com/support/article/SLN322626	H-DEL-XPS_-191020/232
elecom					
wrc-2533gst2					
N/A	06-Oct-20	8.3	ELECOM LAN routers (WRC-2533GST2 firmware versions prior to v1.14, WRC-1900GST2 firmware versions prior to v1.14, WRC-1750GST2 firmware versions prior to v1.14,	N/A	H-ELE-WRC--191020/233

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			and WRC-1167GST2 firmware versions prior to v1.10) allow an attacker on the same network segment to execute arbitrary OS commands with a root privilege via unspecified vectors. **CVE ID : CVE-2020-5634**		
wrc-1900gst2					
N/A	06-Oct-20	8.3	ELECOM LAN routers (WRC-2533GST2 firmware versions prior to v1.14, WRC-1900GST2 firmware versions prior to v1.14, WRC-1750GST2 firmware versions prior to v1.14, and WRC-1167GST2 firmware versions prior to v1.10) allow an attacker on the same network segment to execute arbitrary OS commands with a root privilege via unspecified vectors. **CVE ID : CVE-2020-5634**	N/A	H-ELE-WRC--191020/234
wrc-1750gst2					
N/A	06-Oct-20	8.3	ELECOM LAN routers (WRC-2533GST2 firmware versions prior to v1.14, WRC-1900GST2 firmware versions prior to v1.14, WRC-1750GST2 firmware versions prior to v1.14, and WRC-1167GST2 firmware versions prior to v1.10) allow an attacker on the same network segment to execute	N/A	H-ELE-WRC--191020/235

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			arbitrary OS commands with a root privilege via unspecified vectors. **CVE ID : CVE-2020-5634**		
wrc-1167gst2					
N/A	06-Oct-20	8.3	ELECOM LAN routers (WRC-2533GST2 firmware versions prior to v1.14, WRC-1900GST2 firmware versions prior to v1.14, WRC-1750GST2 firmware versions prior to v1.14, and WRC-1167GST2 firmware versions prior to v1.10) allow an attacker on the same network segment to execute arbitrary OS commands with a root privilege via unspecified vectors. **CVE ID : CVE-2020-5634**	N/A	H-ELE-WRC--191020/236
hpe					
kvm_ip_console_switch_g2					
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	02-Oct-20	3.5	A remote stored xss vulnerability was discovered in HPE KVM IP Console Switches version(s): G2 4x1Ex32 Prior to 2.8.3. **CVE ID : CVE-2020-24627**	N/A	H-HPE-KVM_-191020/237
Improper Control of Generation of Code ('Code Injection')	02-Oct-20	6.5	A remote code injection vulnerability was discovered in HPE KVM IP Console Switches version(s): G2 4x1Ex32 Prior to 2.8.3. **CVE ID : CVE-2020-24628**	N/A	H-HPE-KVM_-191020/238

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
msi					
ambientlink_mslo64					
Out-of-bounds Write	02-Oct-20	7.2	The MSI AmbientLink MsIo64 driver 1.0.0.8 has a Buffer Overflow (0x80102040, 0x80102044, 0x80102050,and 0x80102054). **CVE ID : CVE-2020-17382**	N/A	H-MSI-AMBI-191020/239
sierawireless					
airlink_es440					
Improper Input Validation	06-Oct-20	7.2	Lack of input sanitization in UpdateRebootMgr service of ALEOS 4.11 and later allow an escalation to root from a low-privilege process. **CVE ID : CVE-2020-8781**	https://source.sierrawireless.com/resources/security-bulletins/sierra-wireless-technical-bulletin---swi-psa-2020-005/	H-SIE-AIRL-191020/240
N/A	06-Oct-20	7.5	Unauthenticated RPC server on ALEOS before 4.4.9, 4.9.5, and 4.14.0 allows remote code execution. **CVE ID : CVE-2020-8782**	https://source.sierrawireless.com/resources/security-bulletins/sierra-wireless-technical-bulletin---swi-psa-2020-005/	H-SIE-AIRL-191020/241
airlink_es450					
Improper Input Validation	06-Oct-20	7.2	Lack of input sanitization in UpdateRebootMgr service of ALEOS 4.11 and	https://source.sierrawireless.com/res	H-SIE-AIRL-191020/242

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			later allow an escalation to root from a low-privilege process. **CVE ID : CVE-2020-8781**	ources/security-bulletins/sierra-wireless-technical-bulletin---swi-psa-2020-005/	
N/A	06-Oct-20	7.5	Unauthenticated RPC server on ALEOS before 4.4.9, 4.9.5, and 4.14.0 allows remote code execution. **CVE ID : CVE-2020-8782**	https://source.sierrawireless.com/resources/security-bulletins/sierra-wireless-technical-bulletin---swi-psa-2020-005/	H-SIE-AIRL-191020/243
airlink_gx400					
Improper Input Validation	06-Oct-20	7.2	Lack of input sanitization in UpdateRebootMgr service of ALEOS 4.11 and later allow an escalation to root from a low-privilege process. **CVE ID : CVE-2020-8781**	https://source.sierrawireless.com/resources/security-bulletins/sierra-wireless-technical-bulletin---swi-psa-2020-005/	H-SIE-AIRL-191020/244
N/A	06-Oct-20	7.5	Unauthenticated RPC server on ALEOS before 4.4.9, 4.9.5, and 4.14.0 allows remote code execution. **CVE ID : CVE-2020-8782**	https://source.sierrawireless.com/resources/security-bulletins/sierra-wireless-technical-bulletin---	H-SIE-AIRL-191020/245

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
				swi-psa-2020-005/	
airlink_gx440					
Improper Input Validation	06-Oct-20	7.2	Lack of input sanitization in UpdateRebootMgr service of ALEOS 4.11 and later allow an escalation to root from a low-privilege process. **CVE ID : CVE-2020-8781**	https://source.sierrawireless.com/resources/security-bulletins/sierra-wireless-technical-bulletin---swi-psa-2020-005/	H-SIE-AIRL-191020/246
N/A	06-Oct-20	7.5	Unauthenticated RPC server on ALEOS before 4.4.9, 4.9.5, and 4.14.0 allows remote code execution. **CVE ID : CVE-2020-8782**	https://source.sierrawireless.com/resources/security-bulletins/sierra-wireless-technical-bulletin---swi-psa-2020-005/	H-SIE-AIRL-191020/247
airlink_gx450					
Improper Input Validation	06-Oct-20	7.2	Lack of input sanitization in UpdateRebootMgr service of ALEOS 4.11 and later allow an escalation to root from a low-privilege process. **CVE ID : CVE-2020-8781**	https://source.sierrawireless.com/resources/security-bulletins/sierra-wireless-technical-bulletin---swi-psa-2020-005/	H-SIE-AIRL-191020/248
N/A	06-Oct-20	7.5	Unauthenticated RPC server on ALEOS before	https://source.sierrawire	H-SIE-AIRL-191020/249

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			4.4.9, 4.9.5, and 4.14.0 allows remote code execution. **CVE ID : CVE-2020-8782**	less.com/resources/security-bulletins/sierra-wireless-technical-bulletin---swi-psa-2020-005/	
airlink_ls300					
Improper Input Validation	06-Oct-20	7.2	Lack of input sanitization in UpdateRebootMgr service of ALEOS 4.11 and later allow an escalation to root from a low-privilege process. **CVE ID : CVE-2020-8781**	https://source.sierrawireless.com/resources/security-bulletins/sierra-wireless-technical-bulletin---swi-psa-2020-005/	H-SIE-AIRL-191020/250
N/A	06-Oct-20	7.5	Unauthenticated RPC server on ALEOS before 4.4.9, 4.9.5, and 4.14.0 allows remote code execution. **CVE ID : CVE-2020-8782**	https://source.sierrawireless.com/resources/security-bulletins/sierra-wireless-technical-bulletin---swi-psa-2020-005/	H-SIE-AIRL-191020/251
airlink_lx40					
Improper Input Validation	06-Oct-20	7.2	Lack of input sanitization in UpdateRebootMgr service of ALEOS 4.11 and later allow an escalation to root from a low-privilege process.	https://source.sierrawireless.com/resources/security-bulletins/sierra-wireless-	H-SIE-AIRL-191020/252

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2020-8781	technical-bulletin---swi-psa-2020-005/	
N/A	06-Oct-20	7.5	Unauthenticated RPC server on ALEOS before 4.4.9, 4.9.5, and 4.14.0 allows remote code execution. **CVE ID : CVE-2020-8782**	https://source.sierrawireless.com/resources/security-bulletins/sierra-wireless-technical-bulletin---swi-psa-2020-005/	H-SIE-AIRL-191020/253
airlink_lx60					
Improper Input Validation	06-Oct-20	7.2	Lack of input sanitization in UpdateRebootMgr service of ALEOS 4.11 and later allow an escalation to root from a low-privilege process. **CVE ID : CVE-2020-8781**	https://source.sierrawireless.com/resources/security-bulletins/sierra-wireless-technical-bulletin---swi-psa-2020-005/	H-SIE-AIRL-191020/254
N/A	06-Oct-20	7.5	Unauthenticated RPC server on ALEOS before 4.4.9, 4.9.5, and 4.14.0 allows remote code execution. **CVE ID : CVE-2020-8782**	https://source.sierrawireless.com/resources/security-bulletins/sierra-wireless-technical-bulletin---swi-psa-2020-005/	H-SIE-AIRL-191020/255
airlink_mp70					

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Improper Input Validation	06-Oct-20	7.2	Lack of input sanitization in UpdateRebootMgr service of ALEOS 4.11 and later allow an escalation to root from a low-privilege process. **CVE ID : CVE-2020-8781**	https://source.sierrawireless.com/resources/security-bulletins/sierra-wireless-technical-bulletin---swi-psa-2020-005/	H-SIE-AIRL-191020/256
N/A	06-Oct-20	7.5	Unauthenticated RPC server on ALEOS before 4.4.9, 4.9.5, and 4.14.0 allows remote code execution. **CVE ID : CVE-2020-8782**	https://source.sierrawireless.com/resources/security-bulletins/sierra-wireless-technical-bulletin---swi-psa-2020-005/	H-SIE-AIRL-191020/257
airlink_mp70e					
Improper Input Validation	06-Oct-20	7.2	Lack of input sanitization in UpdateRebootMgr service of ALEOS 4.11 and later allow an escalation to root from a low-privilege process. **CVE ID : CVE-2020-8781**	https://source.sierrawireless.com/resources/security-bulletins/sierra-wireless-technical-bulletin---swi-psa-2020-005/	H-SIE-AIRL-191020/258
N/A	06-Oct-20	7.5	Unauthenticated RPC server on ALEOS before 4.4.9, 4.9.5, and 4.14.0 allows remote code execution.	https://source.sierrawireless.com/resources/security-bulletins/sie	H-SIE-AIRL-191020/259

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2020-8782	rra-wireless-technical-bulletin---swi-psa-2020-005/	
airlink_rv50					
Improper Input Validation	06-Oct-20	7.2	Lack of input sanitization in UpdateRebootMgr service of ALEOS 4.11 and later allow an escalation to root from a low-privilege process. **CVE ID : CVE-2020-8781**	https://source.sierrawireless.com/resources/security-bulletins/sierra-wireless-technical-bulletin---swi-psa-2020-005/	H-SIE-AIRL-191020/260
N/A	06-Oct-20	7.5	Unauthenticated RPC server on ALEOS before 4.4.9, 4.9.5, and 4.14.0 allows remote code execution. **CVE ID : CVE-2020-8782**	https://source.sierrawireless.com/resources/security-bulletins/sierra-wireless-technical-bulletin---swi-psa-2020-005/	H-SIE-AIRL-191020/261
airlink_rv50x					
Improper Input Validation	06-Oct-20	7.2	Lack of input sanitization in UpdateRebootMgr service of ALEOS 4.11 and later allow an escalation to root from a low-privilege process. **CVE ID : CVE-2020-8781**	https://source.sierrawireless.com/resources/security-bulletins/sierra-wireless-technical-bulletin---swi-psa-	H-SIE-AIRL-191020/262

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
				2020-005/	
N/A	06-Oct-20	7.5	Unauthenticated RPC server on ALEOS before 4.4.9, 4.9.5, and 4.14.0 allows remote code execution. **CVE ID : CVE-2020-8782**	https://source.sierrawireless.com/resources/security-bulletins/sierra-wireless-technical-bulletin---swi-psa-2020-005/	H-SIE-AIRL-191020/263
airlink_rv55					
Improper Input Validation	06-Oct-20	7.2	Lack of input sanitization in UpdateRebootMgr service of ALEOS 4.11 and later allow an escalation to root from a low-privilege process. **CVE ID : CVE-2020-8781**	https://source.sierrawireless.com/resources/security-bulletins/sierra-wireless-technical-bulletin---swi-psa-2020-005/	H-SIE-AIRL-191020/264
N/A	06-Oct-20	7.5	Unauthenticated RPC server on ALEOS before 4.4.9, 4.9.5, and 4.14.0 allows remote code execution. **CVE ID : CVE-2020-8782**	https://source.sierrawireless.com/resources/security-bulletins/sierra-wireless-technical-bulletin---swi-psa-2020-005/	H-SIE-AIRL-191020/265
teltonika-networks					
trb245					
Server-Side Request	01-Oct-20	4	Server-Side Request Forgery in Teltonika	N/A	H-TEL-TRB2-

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Forgery (SSRF)			firmware TRB2_R_00.02.04.3 allows a low privileged user to cause the application to perform HTTP GET requests to arbitrary URLs. **CVE ID : CVE-2020-5784**		191020/266
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	01-Oct-20	4.3	Insufficient output sanitization in Teltonika firmware TRB2_R_00.02.04.3 allows an unauthenticated attacker to conduct reflected cross-site scripting via a crafted 'action' or 'pkg_name' parameter. **CVE ID : CVE-2020-5785**	N/A	H-TEL-TRB2-191020/267
Cross-Site Request Forgery (CSRF)	01-Oct-20	6.8	Cross-site request forgery in Teltonika firmware TRB2_R_00.02.04.3 allows a remote attacker to perform sensitive application actions by tricking legitimate users into clicking a crafted link. **CVE ID : CVE-2020-5786**	N/A	H-TEL-TRB2-191020/268
Improper Limitation of a Pathname to a Restricted Directory ('Path Traversal')	01-Oct-20	8.5	Relative Path Traversal in Teltonika firmware TRB2_R_00.02.04.3 allows a remote, authenticated attacker to delete arbitrary files on disk via the admin/services/packages/remove action. **CVE ID : CVE-2020-5787**	N/A	H-TEL-TRB2-191020/269
Improper Limitation of a Pathname to a	01-Oct-20	8.5	Relative Path Traversal in Teltonika firmware TRB2_R_00.02.04.3 allows	N/A	H-TEL-TRB2-

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Restricted Directory ('Path Traversal')			a remote, authenticated attacker to delete arbitrary files on disk via the admin/system/admin/certificates/delete action. **CVE ID : CVE-2020-5788**		191020/270
Improper Limitation of a Pathname to a Restricted Directory ('Path Traversal')	01-Oct-20	4	Relative Path Traversal in Teltonika firmware TRB2_R_00.02.04.3 allows a remote, authenticated attacker to read the contents of arbitrary files on disk. **CVE ID : CVE-2020-5789**	N/A	H-TEL-TRB2-191020/271
wavlink					
wn530h4					
Cross-Site Request Forgery (CSRF)	02-Oct-20	7.8	CSRF vulnerabilities in the /cgi-bin/ directory of the WAVLINK WN530H4 M30H4.V5030.190403 allow an attacker to remotely access router endpoints, because these endpoints do not contain CSRF tokens. If a user is authenticated in the router portal, then this attack will work. **CVE ID : CVE-2020-12123**	N/A	H-WAV-WN53-191020/272
Improper Neutralization of Special Elements used in an OS Command ('OS Command Injection')	02-Oct-20	10	A remote command-line injection vulnerability in the /cgi-bin/live_api.cgi endpoint of the WAVLINK WN530H4 M30H4.V5030.190403 allows an attacker to execute arbitrary Linux commands as root without	N/A	H-WAV-WN53-191020/273

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			authentication. **CVE ID : CVE-2020-12124**		
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	02-Oct-20	10	A remote buffer overflow vulnerability in the /cgi-bin/makeRequest.cgi endpoint of the WAVLINK WN530H4 M30H4.V5030.190403 allows an attacker to execute arbitrary machine instructions as root without authentication. **CVE ID : CVE-2020-12125**	N/A	H-WAV-WN53-191020/274
Improper Authentication	02-Oct-20	7.5	Multiple authentication bypass vulnerabilities in the /cgi-bin/ endpoint of the WAVLINK WN530H4 M30H4.V5030.190403 allow an attacker to leak router settings, change configuration variables, and cause denial of service via an unauthenticated endpoint. **CVE ID : CVE-2020-12126**	N/A	H-WAV-WN53-191020/275
Information Exposure	02-Oct-20	5	An information disclosure vulnerability in the /cgi-bin/ExportAllSettings.sh endpoint of the WAVLINK WN530H4 M30H4.V5030.190403 allows an attacker to leak router settings, including cleartext login details, DNS settings, and other sensitive information without authentication. **CVE ID : CVE-2020-12127**	N/A	H-WAV-WN53-191020/276