Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Application					
Accellion					
kiteworks					
Improper Privilege Management	23-Jun-21	4.6	Accellion Kiteworks before 7.3.1 allows a user with Admin privileges to escalate their privileges by generating SSH passwords that allow local access. **CVE ID : CVE-2021-31585**	https://github.com/accellion/CVEs/blob/main/CVE-2021-31585.txt	A-ACC-KITE-020721/1
Improper Neutralization of Special Elements used in an SQL Command ('SQL Injection')	23-Jun-21	6.5	Accellion Kiteworks before 7.4.0 allows an authenticated user to perform SQL Injection via LDAPGroup Search. **CVE ID : CVE-2021-31586**	https://github.com/accellion/CVEs/blob/main/CVE-2021-31586.txt	A-ACC-KITE-020721/2
admincolumns					
admin_columns					
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	21-Jun-21	3.5	The Admin Columns Free WordPress plugin before 4.3 and Admin Columns Pro WordPress plugin before 5.5.1, rendered input on the posted pages with improper input validation on the value passed into the field 'Label' parameter, by taking this as an advantage an authenticated attacker can supply a crafted arbitrary	https://wpscan.com/vulnerability/05427156-4d5c-4aeb-add8-1c574fda5c28	A-ADM-ADMI-020721/3

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			script and execute it. **CVE ID : CVE-2021-24366**		
Advantech					
webaccess\\/scada					
Relative Path Traversal	18-Jun-21	6.8	Advantech WebAccess/SCADA Versions 9.0.1 and prior is vulnerable to a directory traversal, which may allow an attacker to remotely read arbitrary files on the file system. **CVE ID : CVE-2021-32954**	N/A	A-ADV-WEBA-020721/4
URL Redirection to Untrusted Site ('Open Redirect')	18-Jun-21	5.8	Advantech WebAccess/SCADA Versions 9.0.1 and prior is vulnerable to redirection, which may allow an attacker to send a maliciously crafted URL that could result in redirecting a user to a malicious webpage. **CVE ID : CVE-2021-32956**	N/A	A-ADV-WEBA-020721/5
Ampache					
ampache					
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	22-Jun-21	3.5	Ampache is an open source web based audio/video streaming application and file manager. Due to a lack of input filtering versions 4.x.y are vulnerable to code injection in random.php. The attack requires user authentication to access the random.php page unless the site is running in demo mode. This issue has been resolved in 4.4.3. **CVE ID : CVE-2021-32644**	https://github.com/ampache/ampache/security/advisories/GHSA-vqpj-xgw2-r54q, https://github.com/ampache/ampache/commit/c9453841e1b517a1660c3da1efd1fe5d623c93a5	A-AMP-AMPA-020721/6

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Apache					
cxf					
Uncontrolled Resource Consumption	16-Jun-21	5	A vulnerability in the JsonMapObjectReaderWriter of Apache CXF allows an attacker to submit malformed JSON to a web service, which results in the thread getting stuck in an infinite loop, consuming CPU indefinitely. This issue affects Apache CXF versions prior to 3.4.4; Apache CXF versions prior to 3.3.11. **CVE ID : CVE-2021-30468**	http://cxf.apache.org/security-advisories.data/CVE-2021-30468.txt.asc, https://lists.apache.org/thread.html/r4a4b6bc0520b69c18d2a59daa6af84ae49f0c22164dccb8538794459@%3Cdev.cxf.apache.org%3E	A-APA-CXF-020721/7
nuttx					
Integer Overflow or Wraparound	21-Jun-21	7.5	Apache Nuttx Versions prior to 10.1.0 are vulnerable to integer wrap-around in functions malloc, realloc and memalign. This improper memory assignment can lead to arbitrary memory allocation, resulting in unexpected behavior such as a crash or a remote code injection/execution. **CVE ID : CVE-2021-26461**	https://lists.apache.org/thread.html/r806fccf8b003ae812d807c6c7d97950d44ed29b2713418cbe3f2bddd%40%3Cdev.nuttx.apache.org%3E	A-APA-NUTT-020721/8
Apereo					
opencast					
Improper Restriction	16-Jun-21	4	Opencast is a free and open source solution for	https://github.com/openc	A-APE-OPEN-

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
of Recursive Entity References in DTDs ('XML Entity Expansion')			automated video capture and distribution. Versions of Opencast prior to 9.6 are vulnerable to the billion laughs attack, which allows an attacker to easily execute a (seemingly permanent) denial of service attack, essentially taking down Opencast using a single HTTP request. To exploit this, users need to have ingest privileges, limiting the group of potential attackers The problem has been fixed in Opencast 9.6. There is no known workaround for this issue. **CVE ID : CVE-2021-32623**	ast/opencast/commit/8ae27da5a6f658011a5741b3210e715b0dc6213e, https://github.com/opencast/opencast/security/advisories/GHSA-9gwx-9cwp-5c2m	020721/9
apollosapp					
data-connector-rock					
Improper Authentication	16-Jun-21	7.5	Apollos Apps is an open source platform for launching church-related apps. In Apollos Apps versions prior to 2.20.0, new user registrations are able to access anyone's account by only knowing their basic profile information (name, birthday, gender, etc). This includes all app functionality within the app, as well as any authenticated links to Rock-based webpages (such as giving and events). There is a patch in version 2.20.0. As a workaround, one can patch one's server by overriding the `create` data source	https://github.com/ApollosProject/apollos-apps/releases/tag/v2.20.0, https://github.com/ApollosProject/apollos-apps/commit/cb5f8f1c0b24f1b215b2bb5eb6f9a8e16d728ce2, https://github.com/ApollosProject/ap	A-APO-DATA-020721/10

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			method on the `People` class. **CVE ID : CVE-2021-32691**	ollos-apps/security/advisories/GHSA-r578-pj6f-r4ff	
asken					
asken					
URL Redirection to Untrusted Site ('Open Redirect')	22-Jun-21	5.8	Improper authorization in handler for custom URL scheme vulnerability in ????????? (asken diet) for Android versions from v.3.0.0 to v.4.2.x allows a remote attacker to lead a user to access an arbitrary website via the vulnerable App. **CVE ID : CVE-2021-20733**	https://www.asken.jp/s/login/?to=/information	A-ASK-ASKE-020721/11
Automattic					
jetpack					
Exposure of Resource to Wrong Sphere	21-Jun-21	5	The Jetpack Carousel module of the JetPack WordPress plugin before 9.8 allows users to create a "carousel" type image gallery and allows users to comment on the images. A security vulnerability was found within the Jetpack Carousel module by nguyenhg_vcs that allowed the comments of non-published page/posts to be leaked. **CVE ID : CVE-2021-24374**	https://wpscan.com/vulnerability/08a8a51c-49d3-4bce-b7e0-e365af1d8f33, https://jetpack.com/2021/06/01/jetpack-9-8-engage-your-audience-with-wordpress-stories/	A-AUT-JETP-020721/12
autoptimize					
autoptimize					

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Unrestricted Upload of File with Dangerous Type	21-Jun-21	7.5	The Autoptimize WordPress plugin before 2.7.8 attempts to delete malicious files (such as .php) form the uploaded archive via the "Import Settings" feature, after its extraction. However, the extracted folders are not checked and it is possible to upload a zip which contained a directory with PHP file in it and then it is not removed from the disk. It is a bypass of CVE-2020-24948 which allows sending a PHP file via the "Import Settings" functionality to achieve Remote Code Execution. **CVE ID : CVE-2021-24376**	https://wpscan.com/vulnerability/93edcc23-894a-46c2-84d2-407dcb64ba1e	A-AUT-AUTO-020721/13
Concurrent Execution using Shared Resource with Improper Synchronization ('Race Condition')	21-Jun-21	6.8	The Autoptimize WordPress plugin before 2.7.8 attempts to remove potential malicious files from the extracted archive uploaded via the 'Import Settings' feature, however this is not sufficient to protect against RCE as a race condition can be achieved in between the moment the file is extracted on the disk but not yet removed. It is a bypass of CVE-2020-24948. **CVE ID : CVE-2021-24377**	https://wpscan.com/vulnerability/85c0a564-2e56-413d-bc3a-1039343207e4	A-AUT-AUTO-020721/14
Improper Neutralization of Input During Web Page Generation	21-Jun-21	3.5	The Autoptimize WordPress plugin before 2.7.8 does not check for malicious files such as .html in the archive uploaded via the 'Import Settings' feature. As a result,	https://wpscan.com/vulnerability/375bd694-1a30-41af-bbd4-8a8ee54f0db	A-AUT-AUTO-020721/15

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
('Cross-site Scripting')			it is possible for a high privilege user to upload a malicious file containing JavaScript code inside an archive which will execute when a victim visits index.html inside the plugin directory. **CVE ID : CVE-2021-24378**	f	
Avaya					
aura_utility_services					
N/A	24-Jun-21	2.1	** UNSUPPORTED WHEN ASSIGNED ** An information disclosure vulnerability was discovered in the directory and file management of Avaya Aura Utility Services. This vulnerability may potentially allow any local user to access system functionality and configuration information that should only be available to a privileged user. Affects all 7.x versions of Avaya Aura Utility Services. **CVE ID : CVE-2021-25649**	https://support.avaya.com/css/P8/documents/101072728	A-AVA-AURA-020721/16
Improper Privilege Management	24-Jun-21	4.6	** UNSUPPORTED WHEN ASSIGNED ** A privilege escalation vulnerability was discovered in Avaya Aura Utility Services that may potentially allow a local user to execute specially crafted scripts as a privileged user. Affects all 7.x versions of Avaya Aura Utility Services. **CVE ID : CVE-2021-25650**	https://support.avaya.com/css/P8/documents/101072728	A-AVA-AURA-020721/17

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Improper Privilege Management	24-Jun-21	4.6	** UNSUPPORTED WHEN ASSIGNED ** A privilege escalation vulnerability was discovered in Avaya Aura Utility Services that may potentially allow a local user to escalate privileges. Affects all 7.x versions of Avaya Aura Utility Services. **CVE ID : CVE-2021-25651**	https://support.avaya.com/css/P8/documents/101072728	A-AVA-AURA-020721/18
ayecode					
getpaid					
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	21-Jun-21	3.5	In the GetPaid WordPress plugin before 2.3.4, users with the contributor role and above can create a new Payment Form, however the Label and Help Text input fields were not getting sanitized properly. So it was possible to inject malicious content such as img tags, leading to a Stored Cross-Site Scripting issue which is triggered when the form will be edited, for example when an admin reviews it and could lead to privilege escalation. **CVE ID : CVE-2021-24369**	https://wpscan.com/vulnerability/1d1a731b-78f7-4d97-b40d-80f66700edae	A-AYE-GETP-020721/19
location_manager					
Improper Neutralization of Special Elements used in an SQL Command ('SQL	21-Jun-21	7.5	In the Location Manager WordPress plugin before 2.1.0.10, the AJAX action gd_popular_location_list did not properly sanitise or validate some of its POST parameters, which are then used in a SQL statement,	https://wpgeodirectory.com/downloads/location-manager/, https://wpscan.com/vulnerability/5aff	A-AYE-LOCA-020721/20

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Injection')			leading to unauthenticated SQL Injection issues. **CVE ID : CVE-2021-24361**	50fc-ac96-4076-a07c-bb145ae37025	
ballerina					
ballerina					
Missing Authentication for Critical Function	22-Jun-21	5.8	Ballerina is an open source programming language and platform for cloud application programmers. Ballerina versions 1.2.x and SL releases up to alpha 3 have a potential for a supply chain attack via MiTM against users. Http connections did not make use of TLS and certificate checking was ignored. The vulnerability allows an attacker to substitute or modify packages retrieved from BC thus allowing to inject malicious code into ballerina executables. This has been patched in Ballerina 1.2.14 and Ballerina SwanLake alpha4. **CVE ID : CVE-2021-32700**	https://github.com/ballerina-platform/ballerina-lang/security/advisories/GHSA-f5qg-fqrw-v5ww, https://github.com/ballerina-platform/ballerina-lang/commit/4609ffee1744ecd16aac09303b1783bf0a525816	A-BAL-BALL-020721/21
swan_lake					
Missing Authentication for Critical Function	22-Jun-21	5.8	Ballerina is an open source programming language and platform for cloud application programmers. Ballerina versions 1.2.x and SL releases up to alpha 3 have a potential for a supply chain attack via MiTM against users. Http connections did not make use of TLS and certificate checking was ignored. The	https://github.com/ballerina-platform/ballerina-lang/security/advisories/GHSA-f5qg-fqrw-v5ww, https://github.com/baller	A-BAL-SWAN-020721/22

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			vulnerability allows an attacker to substitute or modify packages retrieved from BC thus allowing to inject malicious code into ballerina executables. This has been patched in Ballerina 1.2.14 and Ballerina SwanLake alpha4. **CVE ID : CVE-2021-32700**	ina-platform/ballerina-lang/commit/4609ffee1744ecd16aac09303b1783bf0a525816	
bindata_project					
bindata					
Uncontrolled Resource Consumption	24-Jun-21	4.3	In the bindata RubyGem before version 2.4.10 there is a potential denial-of-service vulnerability. In affected versions it is very slow for certain classes in BinData to be created. For example BinData::Bit100000, BinData::Bit100001, BinData::Bit100002, BinData::Bit<N>. In combination with <user_input>.constantize there is a potential for a CPU-based DoS. In version 2.4.10 bindata improved the creation time of Bits and Integers. **CVE ID : CVE-2021-32823**	https://github.com/rubysec/ruby-advisory-db/issues/476, https://github.com/dmendel/bindata/commit/d99f050b88337559be2cb35906c1f8da49531323	A-BIN-BIND-020721/23
checksec					
canopy					
Improper Neutralization of Input During Web Page	18-Jun-21	3.5	CheckSec Canopy before 3.5.2 allows XSS attacks against the login page via the LOGIN_PAGE_DISCLAIMER parameter.	N/A	A-CHE-CANO-020721/24

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Generation ('Cross-site Scripting')			**CVE ID : CVE-2021-34815**		
Cisco					
anyconnect_secure_mobility_client					
Time-of-check Time-of-use (TOCTOU) Race Condition	16-Jun-21	6.2	A vulnerability in the DLL loading mechanism of Cisco AnyConnect Secure Mobility Client for Windows could allow an authenticated, local attacker to perform a DLL hijacking attack on an affected device if the VPN Posture (HostScan) Module is installed on the AnyConnect client. This vulnerability is due to a race condition in the signature verification process for DLL files that are loaded on an affected device. An attacker could exploit this vulnerability by sending a series of crafted interprocess communication (IPC) messages to the AnyConnect process. A successful exploit could allow the attacker to execute arbitrary code on the affected device with SYSTEM privileges. To exploit this vulnerability, the attacker must have valid credentials on the Windows system. **CVE ID : CVE-2021-1567**	https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-anyconnect-pos-dll-ff8j6dFv	A-CIS-ANYC-020721/25
Memory Allocation with Excessive Size Value	16-Jun-21	2.1	A vulnerability in Cisco AnyConnect Secure Mobility Client for Windows could allow an authenticated, local attacker to cause a denial of	https://tools.cisco.com/security/center/content/CiscoSecurityAd	A-CIS-ANYC-020721/26

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			service (DoS) condition on an affected system. This vulnerability is due to uncontrolled memory allocation. An attacker could exploit this vulnerability by copying a crafted file to a specific folder on the system. A successful exploit could allow the attacker to crash the VPN Agent service when the affected application is launched, causing it to be unavailable to all users of the system. To exploit this vulnerability, the attacker must have valid credentials on a multiuser Windows system. **CVE ID : CVE-2021-1568**	visory/cisco-sa-anyconnect-dos-hMhyDfb8	
email_security_appliance					
Improper Certificate Validation	16-Jun-21	5.8	A vulnerability in the Cisco Advanced Malware Protection (AMP) for Endpoints integration of Cisco AsyncOS for Cisco Email Security Appliance (ESA) and Cisco Web Security Appliance (WSA) could allow an unauthenticated, remote attacker to intercept traffic between an affected device and the AMP servers. This vulnerability is due to improper certificate validation when an affected device establishes TLS connections. A man-in-the-middle attacker could exploit this vulnerability by sending	https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-esa-wsa-cert-vali-n8L97RW	A-CIS-EMAI-020721/27

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			a crafted TLS packet to an affected device. A successful exploit could allow the attacker to spoof a trusted host and then extract sensitive information or alter certain API requests. **CVE ID : CVE-2021-1566**		
jabber					
N/A	16-Jun-21	4	Multiple vulnerabilities in Cisco Jabber for Windows, Cisco Jabber for Mac, and Cisco Jabber for mobile platforms could allow an attacker to access sensitive information or cause a denial of service (DoS) condition. For more information about these vulnerabilities, see the Details section of this advisory. **CVE ID : CVE-2021-1569**	https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-jabber-GuC5mLwG	A-CIS-JABB-020721/28
Improper Input Validation	16-Jun-21	4	Multiple vulnerabilities in Cisco Jabber for Windows, Cisco Jabber for Mac, and Cisco Jabber for mobile platforms could allow an attacker to access sensitive information or cause a denial of service (DoS) condition. For more information about these vulnerabilities, see the Details section of this advisory. **CVE ID : CVE-2021-1570**	https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-jabber-GuC5mLwG	A-CIS-JABB-020721/29
meeting_server					
Improper Input	16-Jun-21	4	A vulnerability in the API of Cisco Meeting Server could	https://tools.cisco.com/se	A-CIS-MEET-020721/30

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Validation			allow an authenticated, remote attacker to cause a denial of service (DoS) condition on an affected device. This vulnerability exists because requests that are sent to the API are not properly validated. An attacker could exploit this vulnerability by sending a malicious request to the API. A successful exploit could allow the attacker to cause all participants on a call to be disconnected, resulting in a DoS condition. **CVE ID : CVE-2021-1524**	curity/center/content/CiscoSecurityAdvisory/cisco-sa-meetingserver-dos-NzVWMMQT	
web_security_appliance					
Improper Certificate Validation	16-Jun-21	5.8	A vulnerability in the Cisco Advanced Malware Protection (AMP) for Endpoints integration of Cisco AsyncOS for Cisco Email Security Appliance (ESA) and Cisco Web Security Appliance (WSA) could allow an unauthenticated, remote attacker to intercept traffic between an affected device and the AMP servers. This vulnerability is due to improper certificate validation when an affected device establishes TLS connections. A man-in-the-middle attacker could exploit this vulnerability by sending a crafted TLS packet to an affected device. A successful exploit could allow the	https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-esa-wsa-cert-vali-n8L97RW	A-CIS-WEB_-020721/31

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			attacker to spoof a trusted host and then extract sensitive information or alter certain API requests. **CVE ID : CVE-2021-1566**		
Citrix					
cloud_connector					
Insecure Storage of Sensitive Information	16-Jun-21	5	Citrix Cloud Connector before 6.31.0.62192 suffers from insecure storage of sensitive information due to sensitive information being stored in the Citrix Cloud Connector installation log files. Such information could be used by an malicious actor to access a Citrix Cloud environment. This issue affects all versions of Citrix Cloud Connector that were installed by passing secure client parameters for installation via the command line. The issue does not affect Citrix Cloud Connector if it was installed using the interactive installer or where a parameter file was used with the command-line installer. **CVE ID : CVE-2021-22914**	https://support.citrix.com/article/CTX316690	A-CIT-CLOU-020721/32
cleo					
lexicom					
Improper Limitation of a Pathname to a Restricted Directory	18-Jun-21	7.5	An issue was discovered in Cleo LexiCom 5.5.0.0. Within the AS2 message, the sender can specify a filename. This filename can include path-traversal characters, allowing	N/A	A-CLE-LEXI-020721/33

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
('Path Traversal')			the file to be written to an arbitrary location on disk. **CVE ID : CVE-2021-33576**		
Incorrect Authorization	18-Jun-21	5	An issue was discovered in Cleo LexiCom 5.5.0.0. The requirement for the sender of an AS2 message to identify themselves (via encryption and signing of the message) can be bypassed by changing the Content-Type of the message to text/plain. **CVE ID : CVE-2021-33577**	N/A	A-CLE-LEXI-020721/34
Codecabin					
wp_google_maps					
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	21-Jun-21	3.5	The WP Google Maps WordPress plugin before 8.1.12 did not sanitise, validate of escape the Map Name when output in the Map List of the admin dashboard, leading to an authenticated Stored Cross-Site Scripting issue **CVE ID : CVE-2021-24383**	https://wpscan.com/vulnerability/1270588c-53fe-447e-b83c-1b877dc7a954	A-COD-WP_G-020721/35
collne					
welcart					
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	22-Jun-21	4.3	Cross-site scripting vulnerability in Welcart e-Commerce versions prior to 2.2.4 allows remote attackers to inject arbitrary script or HTML via unspecified vectors. **CVE ID : CVE-2021-20734**	https://www.welcart.com/archives/14039.html	A-COL-WELC-020721/36
color-string_project					
color-string					

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Allocation of Resources Without Limits or Throttling	21-Jun-21	5	A Regular Expression Denial of Service (ReDOS) vulnerability was discovered in Color-String version 1.5.5 and below which occurs when the application is provided and checks a crafted invalid HWB string. **CVE ID : CVE-2021-29060**	https://github.com/yetingli/PoCs/blob/main/CVE-2021-29060/Color-String.md, https://github.com/Qix-/color-string/commit/0789e21284c33d89ebc4ab4ca6f759b9375ac9d3	A-COL-COLO-020721/37
connectwise					
automate					
Improper Restriction of XML External Entity Reference	21-Jun-21	7.5	An XXE vulnerability exists in ConnectWise Automate before 2021.0.6.132. **CVE ID : CVE-2021-35066**	https://www.connectwise.com/company/trust/security-bulletins, https://home.connectwise.com/securityBulletin/60cc8c63508a120001cb6e8d	A-CON-AUTO-020721/38
connectwise_automate					
Improper Neutralization of Special Elements used in an SQL Command	17-Jun-21	5	An issue was discovered in ConnectWise Automate before 2021.5. A blind SQL injection vulnerability exists in core agent inventory communication that can enable an attacker to extract	https://home.connectwise.com/securityBulletin/609a9dd75cb8450001e85369,	A-CON-CONN-020721/39

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
('SQL Injection')			database information or administrative credentials from an instance via crafted monitor status responses. **CVE ID : CVE-2021-32582**	https://www.connectwise.com/company/trust/security-bulletins	
Contao					
contao					
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	23-Jun-21	4.3	Contao 4.5.x through 4.9.x before 4.9.16, and 4.10.x through 4.11.x before 4.11.5, allows XSS. It is possible to inject code into the tl_log table that will be executed in the browser when the system log is called in the back end. **CVE ID : CVE-2021-35210**	https://github.com/contao/contao/security/advisories/GHSA-h58v-c6rf-g9f7, https://contao.org/en/security-advisories/cross-site-scripting-in-the-system-log-2021.html	A-CON-CONT-020721/40
djvulibre_project					
djvulibre					
Out-of-bounds Write	24-Jun-21	6.8	A flaw was found in djvulibre-3.5.28 and earlier. An out of bounds write in function DJVU::filter_bv() via crafted djvu file may lead to application crash and other consequences. **CVE ID : CVE-2021-32490**	N/A	A-DJV-DJVU-020721/41
Integer Overflow or Wraparound	24-Jun-21	6.8	A flaw was found in djvulibre-3.5.28 and earlier. An integer overflow in function render() in tools/ddjvu via crafted	N/A	A-DJV-DJVU-020721/42

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			djvu file may lead to application crash and other consequences. **CVE ID : CVE-2021-32491**		
Out-of-bounds Read	24-Jun-21	6.8	A flaw was found in djvulibre-3.5.28 and earlier. An out of bounds read in function DJVU::DataPool::has_data() via crafted djvu file may lead to application crash and other consequences. **CVE ID : CVE-2021-32492**	N/A	A-DJV-DJVU-020721/43
Out-of-bounds Write	24-Jun-21	6.8	A flaw was found in djvulibre-3.5.28 and earlier. A heap buffer overflow in function DJVU::GBitmap::decode() via crafted djvu file may lead to application crash and other consequences. **CVE ID : CVE-2021-32493**	N/A	A-DJV-DJVU-020721/44
Out-of-bounds Write	24-Jun-21	6.8	A flaw was found in djvulibre-3.5.28 and earlier. A Stack overflow in function DJVU::DjVuDocument::get_djvu_file() via crafted djvu file may lead to application crash and other consequences. **CVE ID : CVE-2021-3500**	N/A	A-DJV-DJVU-020721/45
Ec-cube					
business_form_output					
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	22-Jun-21	4.3	Cross-site scripting vulnerability in EC-CUBE Business form output plugin (for EC-CUBE 3.0 series) versions prior to version 1.0.1 allows a remote attacker to inject an arbitrary script via unspecified vector.	N/A	A-EC--BUSI-020721/46

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2021-20742		
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	22-Jun-21	4.3	Cross-site scripting vulnerability in EC-CUBE Category contents plugin (for EC-CUBE 3.0 series) versions prior to version 1.0.1 allows a remote attacker to inject an arbitrary script by leading an administrator or a user to a specially crafted page and to perform a specific operation. **CVE ID : CVE-2021-20744**	https://www.ec-cube.net/products/detail.php?product_id=1070	A-EC--BUSI-020721/47
ec-cube					
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	22-Jun-21	4.3	Cross-site scripting vulnerability in EC-CUBE Business form output plugin (for EC-CUBE 3.0 series) versions prior to version 1.0.1 allows a remote attacker to inject an arbitrary script via unspecified vector. **CVE ID : CVE-2021-20742**	N/A	A-EC--EC-C-020721/48
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	22-Jun-21	4.3	Cross-site scripting vulnerability in EC-CUBE Email newsletters management plugin (for EC-CUBE 3.0 series) versions prior to version 1.0.4 allows a remote attacker to inject an arbitrary script by leading a user to a specially crafted page and to perform a specific operation. **CVE ID : CVE-2021-20743**	N/A	A-EC--EC-C-020721/49
Improper Neutralization of Input During Web	22-Jun-21	4.3	Cross-site scripting vulnerability in EC-CUBE Category contents plugin (for EC-CUBE 3.0 series) versions	https://www.ec-cube.net/products/detail.	A-EC--EC-C-020721/50

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Page Generation ('Cross-site Scripting')			prior to version 1.0.1 allows a remote attacker to inject an arbitrary script by leading an administrator or a user to a specially crafted page and to perform a specific operation. **CVE ID : CVE-2021-20744**	php?product_id=1070	
email_newsletters_management					
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	22-Jun-21	4.3	Cross-site scripting vulnerability in EC-CUBE Email newsletters management plugin (for EC-CUBE 3.0 series) versions prior to version 1.0.4 allows a remote attacker to inject an arbitrary script by leading a user to a specially crafted page and to perform a specific operation. **CVE ID : CVE-2021-20743**	N/A	A-EC--EMAI-020721/51
Eclipse					
jetty					
Insufficient Session Expiration	22-Jun-21	3.6	For Eclipse Jetty versions <= 9.4.40, <= 10.0.2, <= 11.0.2, if an exception is thrown from the SessionListener#sessionDestroyed() method, then the session ID is not invalidated in the session ID manager. On deployments with clustered sessions and multiple contexts this can result in a session not being invalidated. This can result in an application used on a shared computer being left logged in. **CVE ID : CVE-2021-34428**	https://github.com/eclipse/jetty.project/security/advisories/GHSA-m6cp-vxjx-65j6	A-ECL-JETT-020721/52

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
eic					
e-document_system					
Exposure of Sensitive Information to an Unauthorized Actor	16-Jun-21	5	An issue was discovered in EXCELLENT INFOTEK CORPORATION (EIC) E-document System 3.0. A remote attacker can use kw/auth/bbs/asp/get_user_email_info_bbs.asp to obtain the contact information (name and e-mail address) of everyone in the entire organization. This information can allow remote attackers to perform social engineering or brute force attacks against the system login page. **CVE ID : CVE-2021-34683**	https://www.eic.com.tw/eicHome/pro00.html	A-EIC-E-DO-020721/53
elabftw					
elabftw					
Server-Side Request Forgery (SSRF)	21-Jun-21	4	eLabFTW is an open source electronic lab notebook for research labs. This vulnerability allows an attacker to make GET requests on behalf of the server. It is "blind" because the attacker cannot see the result of the request. Issue has been patched in eLabFTW 4.0.0. **CVE ID : CVE-2021-32698**	https://github.com/elabftw/elabftw/commit/3d2db4d3ad90b0915f29f05aeba41eaaf6a7c726, https://github.com/elabftw/elabftw/security/advisories/GHSA-mh6g-62p8-26m4	A-ELA-ELAB-020721/54
expresstech					
quiz_and_survey_master					

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	20-Jun-21	4.3	The Quiz And Survey Master â€“ Best Quiz, Exam and Survey Plugin WordPress plugin before 7.1.18 did not sanitise or escape its result_id parameter when displaying an existing quiz result page, leading to a reflected Cross-Site Scripting issue. This could allow for privilege escalation by inducing a logged in admin to open a malicious link **CVE ID : CVE-2021-24368**	https://wpscan.com/vulnerability/7f2fda5b-45a5-4fc6-968f-90bc9674c999	A-EXP-QUIZ-020721/55
F-secure					
cloud_protection_for_salesforce					
NULL Pointer Dereference	21-Jun-21	4	A Denial-of-Service (DoS) vulnerability was discovered in F-Secure Linux Security whereby the FSAVD component used in certain F-Secure products can crash while scanning larger packages/fuzzed files. The exploit can be triggered remotely by an attacker. A successful attack will result in Denial-of-Service (DoS) of the Anti-Virus engine. **CVE ID : CVE-2021-33572**	https://www.f-secure.com/en/business/support-and-downloads/security-advisories	A-F-S-CLOU-020721/56
elements_for_microsoft_365					
NULL Pointer Dereference	21-Jun-21	4	A Denial-of-Service (DoS) vulnerability was discovered in F-Secure Linux Security whereby the FSAVD component used in certain F-Secure products can crash while scanning larger packages/fuzzed files. The	https://www.f-secure.com/en/business/support-and-downloads/security-	A-F-S-ELEM-020721/57

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			exploit can be triggered remotely by an attacker. A successful attack will result in Denial-of-Service (DoS) of the Anti-Virus engine. **CVE ID : CVE-2021-33572**	advisories	
endpoint_protection					
NULL Pointer Dereference	21-Jun-21	4	A Denial-of-Service (DoS) vulnerability was discovered in F-Secure Linux Security whereby the FSAVD component used in certain F-Secure products can crash while scanning larger packages/fuzzed files. The exploit can be triggered remotely by an attacker. A successful attack will result in Denial-of-Service (DoS) of the Anti-Virus engine. **CVE ID : CVE-2021-33572**	https://www.f-secure.com/en/business/support-and-downloads/security-advisories	A-F-S-ENDP-020721/58
linux_security					
NULL Pointer Dereference	21-Jun-21	4	A Denial-of-Service (DoS) vulnerability was discovered in F-Secure Linux Security whereby the FSAVD component used in certain F-Secure products can crash while scanning larger packages/fuzzed files. The exploit can be triggered remotely by an attacker. A successful attack will result in Denial-of-Service (DoS) of the Anti-Virus engine. **CVE ID : CVE-2021-33572**	https://www.f-secure.com/en/business/support-and-downloads/security-advisories	A-F-S-LINU-020721/59
fisco-bcos					
fisco-bcos					

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Uncontrolled Resource Consumption	24-Jun-21	5	The blockchain node in FISCO-BCOS V2.7.2 may have a bug when dealing with unformatted packet and lead to a crash. A malicious node can send a packet continuously. The packet is in an incorrect format and cannot be decoded by the node correctly. As a result, the node may consume the memory sustainably and crash. More details are shown at: https://github.com/FISCO-BCOS/FISCO-BCOS/issues/1951 **CVE ID : CVE-2021-35041**	https://github.com/FISCO-BCOS/FISCO-BCOS/issues/1951	A-FIS-FISC-020721/60
Fogproject					
fogproject					
Unrestricted Upload of File with Dangerous Type	16-Jun-21	6.5	FOGProject v1.5.9 is affected by a File Upload RCE (Authenticated). **CVE ID : CVE-2021-32243**	N/A	A-FOG-FOGP-020721/61
Foxitsoftware					
foxit_reader					
Access of Resource Using Incompatible Type ('Type Confusion')	16-Jun-21	6.8	This vulnerability allows remote attackers to execute arbitrary code on affected installations of Foxit PhantomPDF 10.1.3.37598. User interaction is required to exploit this vulnerability in that the target must visit a malicious page or open a malicious file. The specific flaw exists within the handling of XFA templates.	https://www.foxit.com/support/security-bulletins.html	A-FOX-FOXI-020721/62

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			The issue results from the lack of proper validation of user-supplied data, which can result in a type confusion condition. An attacker can leverage this vulnerability to execute code in the context of the current process. Was ZDI-CAN-13531. **CVE ID : CVE-2021-31476**		
phantompdf					
Access of Resource Using Incompatible Type ('Type Confusion')	16-Jun-21	6.8	This vulnerability allows remote attackers to execute arbitrary code on affected installations of Foxit PhantomPDF 10.1.3.37598. User interaction is required to exploit this vulnerability in that the target must visit a malicious page or open a malicious file. The specific flaw exists within the handling of XFA templates. The issue results from the lack of proper validation of user-supplied data, which can result in a type confusion condition. An attacker can leverage this vulnerability to execute code in the context of the current process. Was ZDI-CAN-13531. **CVE ID : CVE-2021-31476**	https://www.foxit.com/support/security-bulletins.html	A-FOX-PHAN-020721/63
Get-simple					
getsimplecms					
Unrestricted Upload of File with Dangerous	23-Jun-21	6.5	Remote Code Execution vulnerability in GetSimpleCMS before 3.3.16 in admin/upload.php via	N/A	A-GET-GETS-020721/64

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Type			phar filess. **CVE ID : CVE-2021-28976**		
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	23-Jun-21	3.5	Cross Site Scripting vulnerability in GetSimpleCMS 3.3.16 in admin/upload.php by adding comments or jpg and other file header information to the content of xla, pages, and gzip files, **CVE ID : CVE-2021-28977**	N/A	A-GET-GETS-020721/65
getastra					
wp_hardening					
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	21-Jun-21	4.3	The WP Hardening â€“ Fix Your WordPress Security WordPress plugin before 1.2.2 did not sanitise or escape the $_SERVER['REQUEST_URI'] before outputting it in an attribute, leading to a reflected Cross-Site Scripting issue. **CVE ID : CVE-2021-24372**	https://wpscan.com/vulnerability/5340ae4e-95ba-4a69-beb1-3459cac17782	A-GET-WP_H-020721/66
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	21-Jun-21	4.3	The WP Hardening â€“ Fix Your WordPress Security WordPress plugin before 1.2.2 did not sanitise or escape the historyvalue GET parameter before outputting it in a Javascript block, leading to a reflected Cross-Site Scripting issue. **CVE ID : CVE-2021-24373**	https://wpscan.com/vulnerability/fcf17278-609f-4f75-8a87-9b4579dee1c8	A-GET-WP_H-020721/67
Gitlab					
gitlab					
Uncontrolled	24-Jun-21	4.3	In the bindata RubyGem	https://githu	A-GIT-GITL-

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Resource Consumption			before version 2.4.10 there is a potential denial-of-service vulnerability. In affected versions it is very slow for certain classes in BinData to be created. For example BinData::Bit100000, BinData::Bit100001, BinData::Bit100002, BinData::Bit<N>. In combination with <user_input>.constantize there is a potential for a CPU-based DoS. In version 2.4.10 bindata improved the creation time of Bits and Integers. **CVE ID : CVE-2021-32823**	b.com/rubysec/ruby-advisory-db/issues/476, https://github.com/dmendel/bindata/commit/d99f050b88337559be2cb35906c1f8da49531323	020721/68
gitpod					
gitpod					
URL Redirection to Untrusted Site ('Open Redirect')	22-Jun-21	5.8	Gitpod before 0.6.0 allows unvalidated redirects. **CVE ID : CVE-2021-35206**	https://github.com/gitpod-io/gitpod/pull/2879#issuecomment-865662372, https://github.com/gitpod-io/gitpod/pull/4567/commits/f78b7d18e509e28e71b65bbd4dfd52c16ca57c18, https://github.com/gitpod-	A-GIT-GITP-020721/69

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
				io/gitpod/commit/8ca431f86ae3a6f9a17afcfed51cdd065fcff1a5	
hashicorp					
nomad					
N/A	17-Jun-21	3.3	HashiCorp Nomad and Nomad Enterprise up to version 1.0.4 bridge networking mode allows ARP spoofing from other bridged tasks on the same node. Fixed in 0.12.12, 1.0.5, and 1.1.0 RC1. **CVE ID : CVE-2021-32575**	https://discuss.hashicorp.com/t/hcsec-2021-14-nomad-bridge-networking-mode-allows-arp-spoofing-from-other-bridged-tasks-on-same-node/24296	A-HAS-NOMA-020721/70
helm					
helm					
Exposure of Sensitive Information to an Unauthorized Actor	16-Jun-21	5	Helm is a tool for managing Charts (packages of pre-configured Kubernetes resources). In versions of helm prior to 3.6.1, a vulnerability exists where the username and password credentials associated with a Helm repository could be passed on to another domain referenced by that Helm repository. This issue has been resolved in 3.6.1. There is a workaround through which one may check for	https://github.com/helm/helm/security/advisories/GHSA-56hp-xqp3-w2jf	A-HEL-HELM-020721/71

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			improperly passed credentials. One may use a username and password for a Helm repository and may audit the Helm repository in order to check for another domain being used that could have received the credentials. In the `index.yaml` file for that repository, one may look for another domain in the `urls` list for the chart versions. If there is another domain found and that chart version was pulled or installed, the credentials would be passed on. **CVE ID : CVE-2021-32690**		
Hitachi					
application_server_v10_manual					
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	22-Jun-21	4.3	Cross-site scripting vulnerability in Hitachi Application Server Help (Hitachi Application Server V10 Manual (Windows) version 10-11-01 and earlier and Hitachi Application Server V10 Manual (UNIX) version 10-11-01 and earlier) allows a remote attacker to inject an arbitrary script via unspecified vectors. **CVE ID : CVE-2021-20741**	https://www.hitachi.co.jp/Prod/comp/soft1/global/security/info/vuls/hitachi-sec-2021-104	A-HIT-APPL-020721/72
IBM					
db2					
Improper Neutralization of Special	16-Jun-21	5	Db2 for Linux, UNIX and Windows (includes Db2 Connect Server) 11.1.4 and	https://exchange.xforce.ibmcloud.com	A-IBM-DB2-020721/73

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Elements in Output Used by a Downstream Component ('Injection')			11.5.5 is vulnerable to a denial of service as the server terminates abnormally when executing a specially crafted SELECT statement. IBM X-Force ID: 200658. **CVE ID : CVE-2021-29702**	/vulnerabilities/200658, https://www.ibm.com/support/pages/node/6463985	
Improper Neutralization of Special Elements used in a Command ('Command Injection')	24-Jun-21	5	Db2 for Linux, UNIX and Windows (includes Db2 Connect Server) is vulnerable to a denial of service as the server terminates abnormally when executing a specially crafted SELECT statement. IBM X-Force ID: 200659. **CVE ID : CVE-2021-29703**	https://www.ibm.com/support/pages/node/6466371, https://exchange.xforce.ibmcloud.com/vulnerabilities/200659	A-IBM-DB2-020721/74
guardium_data_encryption					
Generation of Error Message Containing Sensitive Information	28-Jun-21	5	IBM Guardium Data Encryption (GDE) 4.0.0.4 could allow a remote attacker to obtain sensitive information when a detailed technical error message is returned in the browser. This information could be used in further attacks against the system. IBM X-Force ID: 196212. **CVE ID : CVE-2021-20413**	https://www.ibm.com/support/pages/node/6444037	A-IBM-GUAR-020721/75
resilient_security_orchestration_automation_and_response					
Use of a Broken or Risky Cryptographic Algorithm	16-Jun-21	5	IBM Resilient SOAR V38.0 uses weaker than expected cryptographic algorithms that could allow an attacker to decrypt highly sensitive information. IBM X-Force ID: 199238.	https://www.ibm.com/support/pages/node/6464043, https://exchange.xforce.ibmcloud.com	A-IBM-RESI-020721/76

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2021-20566	/vulnerabilities/199238	
Missing Encryption of Sensitive Data	16-Jun-21	2.1	IBM Resilient SOAR V38.0 could allow a local privileged attacker to obtain sensitive information due to improper or nonexisting encryption.IBM X-Force ID: 199239. **CVE ID : CVE-2021-20567**	https://www.ibm.com/support/pages/node/6464039, https://exchange.xforce.ibmcloud.com/vulnerabilities/199239	A-IBM-RESI-020721/77
security_identity_manager					
Server-Side Request Forgery (SSRF)	16-Jun-21	4	IBM Security Identity Manager 6.0.2 is vulnerable to server-side request forgery (SSRF). By sending a specially crafted request, a remote authenticated attacker could exploit this vulnerability to obtain sensitive data. IBM X-Force ID: 197591. **CVE ID : CVE-2021-20483**	https://exchange.xforce.ibmcloud.com/vulnerabilities/197591, https://www.ibm.com/support/pages/node/6464081	A-IBM-SECU-020721/78
Exposure of Resource to Wrong Sphere	16-Jun-21	3.5	IBM Security Identity Manager 6.0.2 could allow an authenticated malicious user to change the passwords of other users in the Windows AD environment when IBM Security Identity Manager Windows Password Synch Plug-in is deployed and configured. IBM X-Force ID: 197789. **CVE ID : CVE-2021-20488**	https://exchange.xforce.ibmcloud.com/vulnerabilities/197789, https://www.ibm.com/support/pages/node/6464081	A-IBM-SECU-020721/79
security_identity_manager_adapter					
Out-of-bounds	28-Jun-21	4	IBM Security Identity Manager Adapters 6.0 and 7.0	https://www.ibm.com/s	A-IBM-SECU-020721/80

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Write			are vulnerable to a heap based buffer overflow, caused by improper bounds. An authenticared user could overflow the buffer and cause the service to crash. IBM X-Force ID: 197882. **CVE ID : CVE-2021-20494**	upport/pages/node/6465875	
icehrm					
icehrm					
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	22-Jun-21	3.5	A stored cross site scripting (XSS) vulnerability was discovered in Ice Hrm 29.0.0.OS which allows attackers to execute arbitrary web scripts or HTML via a crafted file uploaded into the Document Management tab. The exploit is triggered when a user visits the upload location of the crafted file. **CVE ID : CVE-2021-34243**	N/A	A-ICE-ICEH-020721/81
Cross-Site Request Forgery (CSRF)	22-Jun-21	6.8	A cross site request forgery (CSRF) vulnerability was discovered in Ice Hrm 29.0.0.OS which allows attackers to create new admin accounts or change users' passwords. **CVE ID : CVE-2021-34244**	N/A	A-ICE-ICEH-020721/82
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	22-Jun-21	4.3	Cross site scripting (XSS) vulnerability in Ice Hrm 29.0.0.OS, allows attackers to execute arbitrary code via the parameters to the /app/ endpoint. **CVE ID : CVE-2021-35045**	N/A	A-ICE-ICEH-020721/83

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Session Fixation	22-Jun-21	5.8	A session fixation vulnerability was discovered in Ice Hrm 29.0.0 OS which allows an attacker to hijack a valid user session via a crafted session cookie. **CVE ID : CVE-2021-35046**	N/A	A-ICE-ICEH-020721/84
increments					
qiita_markdown					
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	21-Jun-21	4.3	Increments Qiita::Markdown before 0.34.0 allows XSS via a crafted gist link, a different vulnerability than CVE-2021-28796. **CVE ID : CVE-2021-28833**	N/A	A-INC-QIIT-020721/85
Intel					
brand_verification_tool					
Incorrect Default Permissions	17-Jun-21	4.6	Improper permissions in the installer for the Intel(R) Brand Verification Tool before version 11.0.0.1225 may allow an authenticated user to potentially enable escalation of privilege via local access. **CVE ID : CVE-2021-0143**	https://www.intel.com/content/www/us/en/security-center/advisory/intel-sa-00546.html	A-INT-BRAN-020721/86
is-svg_project					
is-svg					
Allocation of Resources Without Limits or Throttling	21-Jun-21	5	A vulnerability was discovered in IS-SVG version 4.3.1 and below where a Regular Expression Denial of Service (ReDOS) occurs if the application is provided and checks a crafted invalid SVG	https://github.com/yetingli/PoCs/blob/main/CVE-2021-29059/IS-SVG.md	A-IS--IS-S-020721/87

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			string. **CVE ID : CVE-2021-29059**		
jdom					
jdom					
Improper Restriction of XML External Entity Reference	16-Jun-21	5	An XXE issue in SAXBuilder in JDOM through 2.0.6 allows attackers to cause a denial of service via a crafted HTTP request. **CVE ID : CVE-2021-33813**	https://github.com/hunterhacker/jdom/pull/188	A-JDO-JDOM-020721/88
Jenkins					
generic_webhook_trigger					
Improper Restriction of XML External Entity Reference	18-Jun-21	7.5	Jenkins Generic Webhook Trigger Plugin 1.72 and earlier does not configure its XML parser to prevent XML external entity (XXE) attacks. **CVE ID : CVE-2021-21669**	https://www.jenkins.io/security/advisory/2021-06-18/#SECURITY-2330	A-JEN-GENE-020721/89
scriptler					
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	16-Jun-21	3.5	Jenkins Scriptler Plugin 3.2 and earlier does not escape parameter names shown in job configuration forms, resulting in a stored cross-site scripting (XSS) vulnerability exploitable by attackers with Scriptler/Configure permission. **CVE ID : CVE-2021-21667**	https://www.jenkins.io/security/advisory/2021-06-16/#SECURITY-2224	A-JEN-SCRI-020721/90
Improper Neutralization of Input During Web Page Generation	16-Jun-21	3.5	Jenkins Scriptler Plugin 3.1 and earlier does not escape script content, resulting in a stored cross-site scripting (XSS) vulnerability exploitable by attackers with	https://www.jenkins.io/security/advisory/2021-06-16/#SECURI	A-JEN-SCRI-020721/91

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
('Cross-site Scripting')			Scriptler/Configure permission. **CVE ID : CVE-2021-21668**	TY-2390	
jpress					
jpress					
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	18-Jun-21	3.5	An issue was discovered in JPress v3.3.0 and below. There are XSS vulnerabilities in the template module and tag management module. If you log in to the background by means of weak password, the storage XSS vulnerability can occur. **CVE ID : CVE-2021-33347**	N/A	A-JPR-JPRE-020721/92
lutils_project					
lutils					
N/A	17-Jun-21	7.5	All versions of package lutils are vulnerable to Prototype Pollution via the main (merge) function. **CVE ID : CVE-2021-23396**	N/A	A-LUT-LUTI-020721/93
Mantisbt					
mantisbt					
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	17-Jun-21	4.3	An XSS issue was discovered in manage_custom_field_edit_page.php in MantisBT before 2.25.2. Unescaped output of the return parameter allows an attacker to inject code into a hidden input field. **CVE ID : CVE-2021-33557**	https://mantisbt.org/bugs/view.php?id=28552, https://mantisbt.org/blog/archives/mantisbt/699	A-MAN-MANT-020721/94
Matrix					
olm					

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Out-of-bounds Write	16-Jun-21	7.5	Matrix libolm before 3.2.3 allows a malicious Matrix homeserver to crash a client (while it is attempting to retrieve an Olm encrypted room key backup from the homeserver) because olm_pk_decrypt has a stack-based buffer overflow. Remote code execution might be possible for some nonstandard build configurations. **CVE ID : CVE-2021-34813**	https://gitlab.matrix.org/matrix-org/olm/-/releases/3.2.3, https://matrix.org/blog/2021/06/14/adventures-in-fuzzing-libolm, https://gitlab.matrix.org/matrix-org/olm/-/commit/ccc0d122ee1b4d5e5ca4ec1432086be17d5f901b	A-MAT-OLM-020721/95
mcusystem					
mcusystem					
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	18-Jun-21	4.3	The login page in the MCUsystem does not filter with special characters, which allows remote attackers can inject JavaScript without privilege and thus perform reflected XSS attacks. **CVE ID : CVE-2021-32536**	N/A	A-MCU-MCUS-020721/96
mongo-express_project					
mongo-express					
Improper Neutralization of Input During Web Page	21-Jun-21	4.3	mongo-express is a web-based MongoDB admin interface, written with Node.js and express. 1: As mentioned in this issue:	https://github.com/mongo-express/mongo-	A-MON-MONG-020721/97

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Generation ('Cross-site Scripting')			https://github.com/mongo-express/mongo-express/issues/577, when the content of a cell grows larger than supported size, clicking on a row will show full document unescaped, however this needs admin interaction on cell. 2: Data cells identified as media will be rendered as media, without being sanitized. Example of different renders: image, audio, video, etc. As an example of type 1 attack, an unauthorized user who only can send a large amount of data in a field of a document may use a payload with embedded javascript. This could send an export of a collection to the attacker without even an admin knowing. Other types of attacks such as dropping a database\collection are possible. **CVE ID : CVE-2021-21422**	express/commit/f5e0d4931f856f032f22664b5e5901d5950cfd4b, https://github.com/mongo-express/mongo-express/security/advisories/GHSA-7p8h-86p5-wv3p	
Moodle					
moodle					
Incorrect Permission Assignment for Critical Resource	23-Jun-21	9	A command execution vulnerability exists in the default legacy spellchecker plugin in Moodle 3.10. A specially crafted series of HTTP requests can lead to command execution. An attacker must have administrator privileges to	N/A	A-MOO-MOOD-020721/98

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			exploit this vulnerabilities. **CVE ID : CVE-2021-21809**		
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	16-Jun-21	3.5	Cross Site Scripting (XSS) in Moodle 3.10.3 allows remote attackers to execute arbitrary web script or HTML via the "Description" field. **CVE ID : CVE-2021-32244**	N/A	A-MOO-MOOD-020721/99
Mozilla					
firefox					
Integer Overflow or Wraparound	24-Jun-21	6.8	Ports that were written as an integer overflow above the bounds of a 16-bit integer could have bypassed port blocking restrictions when used in the Alt-Svc header. This vulnerability affects Firefox ESR < 78.10, Thunderbird < 78.10, and Firefox < 88. **CVE ID : CVE-2021-29946**	https://www.mozilla.org/security/advisories/mfsa2021-15/, https://www.mozilla.org/security/advisories/mfsa2021-16/, https://www.mozilla.org/security/advisories/mfsa2021-14/, https://bugzilla.mozilla.org/show_bug.cgi?id=1698503	A-MOZ-FIRE-020721/100
Improper Restriction of Operations within the Bounds of a Memory	24-Jun-21	6.8	Mozilla developers and community members reported memory safety bugs present in Firefox 87. Some of these bugs showed evidence of memory corruption and we presume that with enough	https://www.mozilla.org/security/advisories/mfsa2021-16/, https://bugzilla.mozilla.o	A-MOZ-FIRE-020721/101

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Buffer			effort some of these could have been exploited to run arbitrary code. This vulnerability affects Firefox < 88. **CVE ID : CVE-2021-29947**	rg/buglist.cgi?bug_id=1651449%2C1674142%2C1693476%2C1696886%2C1700091	
Concurrent Execution using Shared Resource with Improper Synchronization ('Race Condition')	24-Jun-21	5.1	When Web Render components were destructed, a race condition could have caused undefined behavior, and we presume that with enough effort may have been exploitable to run arbitrary code. This vulnerability affects Firefox < 88.0.1 and Firefox for Android < 88.1.3. **CVE ID : CVE-2021-29952**	https://www.mozilla.org/security/advisories/mfsa2021-20/, https://bugzilla.mozilla.org/show_bug.cgi?id=1704227	A-MOZ-FIRE-020721/102
Exposure of Resource to Wrong Sphere	24-Jun-21	4.3	When a download was initiated, the client did not check whether it was in normal or private browsing mode, which led to private mode cookies being shared in normal browsing mode. This vulnerability affects Firefox for iOS < 34. **CVE ID : CVE-2021-29958**	https://www.mozilla.org/security/advisories/mfsa2021-25/, https://bugzilla.mozilla.org/show_bug.cgi?id=1670127	A-MOZ-FIRE-020721/103
Improper Resource Shutdown or Release	24-Jun-21	4.3	Firefox for Android would become unstable and hard-to-recover when a website opened too many popups. *This bug only affects Firefox for Android. Other operating systems are unaffected.*. This vulnerability affects Firefox < 89. **CVE ID : CVE-2021-29962**	https://www.mozilla.org/security/advisories/mfsa2021-23/, https://bugzilla.mozilla.org/show_bug.cgi?id=1701673	A-MOZ-FIRE-020721/104
Improper	24-Jun-21	6.8	Mozilla developers reported	https://ww	A-MOZ-FIRE-

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Restriction of Operations within the Bounds of a Memory Buffer			memory safety bugs present in Firefox 88. 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 < 89. **CVE ID : CVE-2021-29966**	w.mozilla.org /security/advisories/mfsa2021-23/	020721/105
Improper Restriction of Operations within the Bounds of a Memory Buffer	24-Jun-21	6.8	Mozilla developers reported memory safety bugs present in Firefox 88 and Firefox ESR 78.11. 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 Thunderbird < 78.11, Firefox < 89, and Firefox ESR < 78.11. **CVE ID : CVE-2021-29967**	https://www.mozilla.org/security/advisories/mfsa2021-23/, https://www.mozilla.org/security/advisories/mfsa2021-24/, https://www.mozilla.org/security/advisories/mfsa2021-26/	A-MOZ-FIRE-020721/106
Out-of-bounds Read	24-Jun-21	5.8	When drawing text onto a canvas with WebRender disabled, an out of bounds read could occur. *This bug only affects Firefox on Windows. Other operating systems are unaffected.*. This vulnerability affects Firefox < 89.0.1. **CVE ID : CVE-2021-29968**	https://bugzilla.mozilla.org/show_bug.cgi?id=1712047, https://www.mozilla.org/security/advisories/mfsa2021-27/	A-MOZ-FIRE-020721/107
firefox_esr					
Integer Overflow or	24-Jun-21	6.8	Ports that were written as an integer overflow above the	https://www.mozilla.org	A-MOZ-FIRE-020721/108

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Wraparound			bounds of a 16-bit integer could have bypassed port blocking restrictions when used in the Alt-Svc header. This vulnerability affects Firefox ESR < 78.10, Thunderbird < 78.10, and Firefox < 88. **CVE ID : CVE-2021-29946**	/security/advisories/mfsa2021-15/, https://www.mozilla.org/security/advisories/mfsa2021-16/, https://www.mozilla.org/security/advisories/mfsa2021-14/, https://bugzilla.mozilla.org/show_bug.cgi?id=1698503	
Improper Restriction of Operations within the Bounds of a Memory Buffer	24-Jun-21	6.8	Mozilla developers reported memory safety bugs present in Firefox 88 and Firefox ESR 78.11. 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 Thunderbird < 78.11, Firefox < 89, and Firefox ESR < 78.11. **CVE ID : CVE-2021-29967**	https://www.mozilla.org/security/advisories/mfsa2021-23/, https://www.mozilla.org/security/advisories/mfsa2021-24/, https://www.mozilla.org/security/advisories/mfsa2021-26/	A-MOZ-FIRE-020721/109
thunderbird					
Integer Overflow or Wraparound	24-Jun-21	6.8	Ports that were written as an integer overflow above the bounds of a 16-bit integer could have bypassed port blocking restrictions when used in the Alt-Svc header.	https://www.mozilla.org/security/advisories/mfsa2021-15/, https://ww	A-MOZ-THUN-020721/110

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			This vulnerability affects Firefox ESR < 78.10, Thunderbird < 78.10, and Firefox < 88. **CVE ID : CVE-2021-29946**	w.mozilla.org/security/advisories/mfsa2021-16/, https://www.mozilla.org/security/advisories/mfsa2021-14/, https://bugzilla.mozilla.org/show_bug.cgi?id=1698503	
Cleartext Storage of Sensitive Information	24-Jun-21	5	Thunderbird unprotects a secret OpenPGP key prior to using it for a decryption, signing or key import task. If the task runs into a failure, the secret key may remain in memory in its unprotected state. This vulnerability affects Thunderbird < 78.8.1. **CVE ID : CVE-2021-29950**	https://bugzilla.mozilla.org/show_bug.cgi?id=1673239, https://www.mozilla.org/security/advisories/mfsa2021-17/	A-MOZ-THUN-020721/111
Improper Restriction of Operations within the Bounds of a Memory Buffer	24-Jun-21	6.8	Mozilla developers reported memory safety bugs present in Firefox 88 and Firefox ESR 78.11. 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 Thunderbird < 78.11, Firefox < 89, and Firefox ESR < 78.11. **CVE ID : CVE-2021-29967**	https://www.mozilla.org/security/advisories/mfsa2021-23/, https://www.mozilla.org/security/advisories/mfsa2021-24/, https://www.mozilla.org/security/advisories/mfsa2021-26/	A-MOZ-THUN-020721/112

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
mpmath					
mpmath					
Allocation of Resources Without Limits or Throttling	21-Jun-21	5	A Regular Expression Denial of Service (ReDOS) vulnerability was discovered in Mpmath v1.0.0 when the mpmathify function is called. **CVE ID : CVE-2021-29063**	https://github.com/npm/hosted-git-info/pull/76, https://github.com/yetingli/PoCs/blob/main/CVE-2021-29063/Mpmath.md	A-MPM-MPMA-020721/113
msi					
dragon_center					
Improper Privilege Management	21-Jun-21	7.2	MODAPI.sys in MSI Dragon Center 2.0.104.0 allows low-privileged users to access kernel memory and potentially escalate privileges via a crafted IOCTL 0x9c406104 call. This IOCTL provides the MmMapIoSpace feature for mapping physical memory. **CVE ID : CVE-2021-29337**	https://github.com/rjt-gupta/CVE-2021-29337	A-MSI-DRAG-020721/114
myq-solution					
myq_server					
Improper Neutralization of Special Elements used in an OS Command ('OS Command Injection')	21-Jun-21	9	MyQ Server in MyQ X Smart before 8.2 allows remote code execution by unprivileged users because administrative session data can be read in the %PROGRAMFILES%\MyQ\PHP\Sessions directory. The "Select server file" feature is only intended for	N/A	A-MYQ-MYQ_-020721/115

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			administrators but actually does not require authorization. An attacker can inject arbitrary OS commands (such as commands to create new .php files) via the Task Scheduler component. **CVE ID : CVE-2021-31769**		
neos					
form					
Improper Input Validation	21-Jun-21	5	neos/forms is an open source framework to build web forms. By crafting a special `GET` request containing a valid form state, a form can be submitted without invoking any validators. Form state is secured with an HMAC that is still verified. That means that this issue can only be exploited if Form Finishers cause side effects even if no form values have been sent. Form Finishers can be adjusted in a way that they only execute an action if the submitted form contains some expected data. Alternatively a custom Finisher can be added as first finisher. This regression was introduced with https://github.com/neos/form/commit/049d415295be8d4a0478ccba97dba1bb81649567 **CVE ID : CVE-2021-32697**	https://github.com/neos/form/commit/69de4219b1f58157e2be6b05811463875d75c246, https://github.com/neos/form/security/advisories/GHSA-m5vx-8chx-qvmm, https://github.com/neos/form/commit/049d415295be8d4a0478ccba97dba1bb81649567	A-NEO-FORM-020721/116
Nextcloud					

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
nextcloud					
Uncaught Exception	17-Jun-21	4.3	Nextcloud Android app is the Android client for Nextcloud. In versions prior to 3.15.1, a malicious application on the same device is possible to crash the Nextcloud Android Client due to an uncaught exception. The vulnerability is patched in version 3.15.1. **CVE ID : CVE-2021-32694**	https://github.com/nextcloud/security-advisories/security/advisories/GHSA-h2gm-m374-99vc, https://github.com/nextcloud/android/pull/7919	A-NEX-NEXT-020721/117
Exposure of Sensitive Information to an Unauthorized Actor	17-Jun-21	4.3	Nextcloud Android app is the Android client for Nextcloud. In versions prior to 3.16.1, a malicious app on the same device could have gotten access to the shared preferences of the Nextcloud Android application. This required user-interaction as a victim had to initiate the sharing flow and choose the malicious app. The shared preferences contain some limited private data such as push tokens and the account name. The vulnerability is patched in version 3.16.1. **CVE ID : CVE-2021-32695**	https://github.com/nextcloud/android/pull/8433, https://github.com/nextcloud/security-advisories/security/advisories/GHSA-25m9-cf6c-qf2c	A-NEX-NEXT-020721/118
talk					
Session Fixation	16-Jun-21	4	Nextcloud Talk is a fully on-premises audio/video and chat communication service. Password protected shared chats in Talk before version 9.0.10, 10.0.8 and 11.2.2 did	https://github.com/nextcloud/security-advisories/security/advis	A-NEX-TALK-020721/119

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			not rotate the session cookie after a successful authentication event. It is recommended that the Nextcloud Talk App is upgraded to 9.0.10, 10.0.8 or 11.2.2. No workarounds for this vulnerability are known to exist. **CVE ID : CVE-2021-32676**	ories/GHSA-p6h7-84v4-827r	
octopus					
server					
Improper Neutralization of Special Elements used in an SQL Command ('SQL Injection')	17-Jun-21	4	Affected versions of Octopus Server are prone to an authenticated SQL injection vulnerability in the Events REST API because user supplied data in the API request isn't parameterised correctly. Exploiting this vulnerability could allow unauthorised access to database tables. **CVE ID : CVE-2021-31818**	https://advisories.octopus.com/adv/2021-04---SQL-Injection-in-the-Events-REST-API-(CVE-2021-31818).2013233248.html	A-OCT-SERV-020721/120
opendesign					
drawings_sdk					
Out-of-bounds Write	17-Jun-21	6.8	An out-of-bounds write issue exists in the DXF file-recovering procedure in the Drawings SDK (All versions prior to 2022.4) resulting from the lack of proper validation of user-supplied data. This can result in a write past the end of an allocated buffer and allow attackers to cause a denial-of-service condition or execute	N/A	A-OPE-DRAW-020721/121

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			code in the context of the current process. **CVE ID : CVE-2021-32936**		
Out-of-bounds Read	17-Jun-21	5.8	Drawings SDK (All versions prior to 2022.4) are vulnerable to an out-of-bounds read due to parsing of DWG files resulting from the lack of proper validation of user-supplied data. This can result in a read past the end of an allocated buffer and allows attackers to cause a denial-of service condition or read sensitive information from memory. **CVE ID : CVE-2021-32938**	https://us-cert.cisa.gov/ics/advisories/icsa-21-159-02	A-OPE-DRAW-020721/122
Out-of-bounds Read	17-Jun-21	5.8	An out-of-bounds read issue exists in the DWG file-recovering procedure in the Drawings SDK (All versions prior to 2022.4) resulting from the lack of proper validation of user-supplied data. This can result in a read past the end of an allocated buffer and allow attackers to cause a denial-of-service condition or read sensitive information from memory locations. **CVE ID : CVE-2021-32940**	N/A	A-OPE-DRAW-020721/123
Use After Free	17-Jun-21	6.8	A use-after-free issue exists in the DGN file-reading procedure in the Drawings SDK (All versions prior to 2022.4) resulting from the lack of proper validation of user-supplied data. This can	N/A	A-OPE-DRAW-020721/124

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			result in a memory corruption or arbitrary code execution, allowing attackers to cause a denial-of-service condition or execute code in the context of the current process. **CVE ID : CVE-2021-32944**		
Improper Check for Unusual or Exceptional Conditions	17-Jun-21	6.8	An improper check for unusual or exceptional conditions issue exists within the parsing DGN files from Drawings SDK (Version 2022.4 and prior) resulting from the lack of proper validation of the user-supplied data. This may result in several of out-of-bounds problems and allow attackers to cause a denial-of-service condition or execute code in the context of the current process. **CVE ID : CVE-2021-32946**	N/A	A-OPE-DRAW-020721/125
Out-of-bounds Write	17-Jun-21	6.8	An out-of-bounds write issue exists in the DWG file-reading procedure in the Drawings SDK (All versions prior to 2022.4) resulting from the lack of proper validation of user-supplied data. This can result in a write past the end of an allocated buffer and allow attackers to cause a denial-of-service condition or execute code in the context of the current process. **CVE ID : CVE-2021-32948**	N/A	A-OPE-DRAW-020721/126
Out-of-	17-Jun-21	5.8	An out-of-bounds read issue	N/A	A-OPE-

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
bounds Read			exists within the parsing of DXF files in the Drawings SDK (All versions prior to 2022.4) resulting from the lack of proper validation of user-supplied data. This can result in a read past the end of an allocated buffer and allows attackers to cause a denial-of-service condition or read sensitive information from memory locations. **CVE ID : CVE-2021-32950**		DRAW-020721/127
Out-of-bounds Write	17-Jun-21	6.8	An out-of-bounds write issue exists in the DGN file-reading procedure in the Drawings SDK (Version 2022.4 and prior) resulting from the lack of proper validation of user-supplied data. This can result in a write past the end of an allocated buffer and allow attackers to cause a denial-of-service condition or execute code in the context of the current process. **CVE ID : CVE-2021-32952**	N/A	A-OPE-DRAW-020721/128
opener_project					
opener					
Out-of-bounds Read	17-Jun-21	9.4	An information disclosure vulnerability exists in the Ethernet/IP UDP handler functionality of EIP Stack Group OpENer 2.3 and development commit 8c73bf3. A specially crafted network request can lead to an out-of-bounds read. **CVE ID : CVE-2021-21777**	N/A	A-OPE-OPEN-020721/129

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Oracle					
opengrok					
XML Injection (aka Blind XPath Injection)	23-Jun-21	6.5	Vulnerability in OpenGrok (component: Web App). Versions that are affected are 1.6.7 and prior. Easily exploitable vulnerability allows low privileged attacker with network access via HTTPS to compromise OpenGrok. Successful attacks of this vulnerability can result in takeover of OpenGrok. CVSS 3.1 Base Score 8.8 (Confidentiality, Integrity and Availability impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H). **CVE ID : CVE-2021-2322**	https://www.oracle.com/security-alerts/oracle-open-source-cves-outside-other-oracle-public-documents.html	A-ORA-OPEN-020721/130
ory					
oathkeeper					
Incorrect Authorization	22-Jun-21	4.3	ORY Oathkeeper is an Identity & Access Proxy (IAP) and Access Control Decision API that authorizes HTTP requests based on sets of Access Rules. When you make a request to an endpoint that requires the scope `foo` using an access token granted with that `foo` scope, introspection will be valid and that token will be cached. The problem comes when a second requests to an endpoint that requires the scope `bar` is made before the cache has expired. Whether the token is	https://github.com/ory/oathkeeper/pull/424, https://github.com/ory/oathkeeper/commit/1f9f625c1a49e134ae2299ee95b8cf158feec932, https://github.com/ory/oathkeeper/security/advisories/GHSA-	A-ORY-OATH-020721/131

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			granted or not to the `bar` scope, introspection will be valid. A patch will be released with `v0.38.12-beta.1`. Per default, caching is disabled for the `oauth2_introspection` authenticator. When caching is disabled, this vulnerability does not exist. The cache is checked in [`func (a *AuthenticatorOAuth2Introspection) Authenticate(...)`](https://github.com/ory/oathkeeper/blob/6a31df1c3779425e05db1c2a381166b087cb29a4/pipeline/authn/authenticator_oauth2_introspection.go#L152). From [`tokenFromCache()`](https://github.com/ory/oathkeeper/blob/6a31df1c3779425e05db1c2a381166b087cb29a4/pipeline/authn/authenticator_oauth2_introspection.go#L97) it seems that it only validates the token expiration date, but ignores whether the token has or not the proper scopes. The vulnerability was introduced in PR #424. During review, we failed to require appropriate test coverage by the submitter which is the primary reason that the vulnerability passed the review process. **CVE ID : CVE-2021-32701**	qvp4-rpmr-xwrr	
Otrs					
otrs					

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	16-Jun-21	4.3	There is a XSS vulnerability in the ticket overview screens. It's possible to collect various information by having an e-mail shown in the overview screen. Attack can be performed by sending specially crafted e-mail to the system and it doesn't require any user intraction. This issue affects: OTRS AG ((OTRS)) Community Edition 6.0.x version 6.0.1 and later versions. OTRS AG OTRS 7.0.x version 7.0.26 and prior versions. **CVE ID : CVE-2021-21441**	https://otrs.com/release-notes/otrs-security-advisory-2021-11/	A-OTR-OTRS-020721/132
pagekit					
pagekit					
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	16-Jun-21	3.5	In PageKit v1.0.18, a user can upload SVG files in the file upload portion of the CMS. These SVG files can contain malicious scripts. This file will be uploaded to the system and it will not be stripped or filtered. The user can create a link on the website pointing to "/storage/exp.svg" that will point to http://localhost/pagekit/storage/exp.svg. When a user comes along to click that link, it will trigger a XSS attack. **CVE ID : CVE-2021-32245**	N/A	A-PAG-PAGE-020721/133
Paloaltonetworks					
cortex_xsoar					

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Incorrect Authorization	22-Jun-21	7.5	An improper authorization vulnerability in Palo Alto Networks Cortex XSOAR enables a remote unauthenticated attacker with network access to the Cortex XSOAR server to perform unauthorized actions through the REST API. This issue impacts: Cortex XSOAR 6.1.0 builds later than 1016923 and earlier than 1271064; Cortex XSOAR 6.2.0 builds earlier than 1271065. This issue does not impact Cortex XSOAR 5.5.0, Cortex XSOAR 6.0.0, Cortex XSOAR 6.0.1, or Cortex XSOAR 6.0.2 versions. All Cortex XSOAR instances hosted by Palo Alto Networks are upgraded to resolve this vulnerability. No additional action is required for these instances. **CVE ID : CVE-2021-3044**	https://security.paloaltonetworks.com/CVE-2021-3044	A-PAL-CORT-020721/134
Phpipam					
phpipam					
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	23-Jun-21	4.3	phpIPAM 1.4.3 allows Reflected XSS via app/dashboard/widgets/ipcalc-result.php and app/tools/ip-calculator/result.php of the IP calculator. **CVE ID : CVE-2021-35438**	https://github.com/phpipam/phpipam/issues/3351	A-PHP-PHPI-020721/135
phpmailer_project					
phpmailer					
Unrestricted	16-Jun-21	5.1	PHPMailer before 6.5.0 on	https://githu	A-PHP-

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Upload of File with Dangerous Type			Windows allows remote code execution if lang_path is untrusted data and has a UNC pathname. **CVE ID : CVE-2021-34551**	b.com/PHPMailer/PHPMailer/blob/master/SECURITY.md	PHPM-020721/136
Inclusion of Functionality from Untrusted Control Sphere	17-Jun-21	6.8	PHPMailer 6.4.1 and earlier contain a vulnerability that can result in untrusted code being called (if such code is injected into the host project's scope by other means). If the $patternselect parameter to validateAddress() is set to 'php' (the default, defined by PHPMailer::$validator), and the global namespace contains a function called php, it will be called in preference to the built-in validator of the same name. Mitigated in PHPMailer 6.5.0 by denying the use of simple strings as validator function names. **CVE ID : CVE-2021-3603**	https://github.com/PHPMailer/PHPMailer/commit/45f3c18dc6a2de1cb1bf49b9b249a9ee36a5f7f3, https://www.huntr.dev/bounties/1-PHPMailer/PHPMailer/	A-PHP-PHPM-020721/137
Podsfoundation					
pods					
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	21-Jun-21	3.5	The Pods â€“ Custom Content Types and Fields WordPress plugin before 2.7.27 was vulnerable to an Authenticated Stored Cross-Site Scripting (XSS) security vulnerability within the 'Singular Label' field parameter. **CVE ID : CVE-2021-24338**	https://wpscan.com/vulnerability/d5b015f3-90c7-4d51-a71d-630d60965151, https://www.whitesourcesoftware.com/vulnerab	A-POD-PODS-020721/138

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
				ility-database/CVE-2021-24338	
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	21-Jun-21	3.5	The Pods â€“ Custom Content Types and Fields WordPress plugin before 2.7.27 was vulnerable to an Authenticated Stored Cross-Site Scripting (XSS) security vulnerability within the 'Menu Label' field parameter. **CVE ID : CVE-2021-24339**	https://wpscan.com/vulnerability/8e72236d-f620-4503-a324-dcf49405351b	A-POD-PODS-020721/139
Powerarchiver					
powerarchiver					
Improper Restriction of XML External Entity Reference	21-Jun-21	4.3	The XML parser used in ConeXware PowerArchiver before 20.10.02 allows processing of external entities, which might lead to exfiltration of local files over the network (via an XXE attack). **CVE ID : CVE-2021-28684**	N/A	A-POW-POWE-020721/140
primion-digitek					
secure_8					
Improper Neutralization of Special Elements used in an SQL Command ('SQL Injection')	18-Jun-21	7.5	Secure 8 (Evalos) does not validate user input data correctly, allowing a remote attacker to perform a Blind SQL Injection. An attacker could exploit this vulnerability in order to extract information of users and administrator accounts stored in the database. **CVE ID : CVE-2021-3604**	http://titaniumaics.blogspot.com/2021/06/vulnerabilidad-zero-day-en-primion.html, https://www.incibe-cert.es/en/early-	A-PRI-SECU-020721/141

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
				warning/ics-advisories/primion-digitek-secure-8-sql-injection-vulnerability	
pterodactyl					
wings					
Uncontrolled Resource Consumption	22-Jun-21	2.1	Wings is the control plane software for the open source Pterodactyl game management system. All versions of Pterodactyl Wings prior to `1.4.4` are vulnerable to system resource exhaustion due to improper container process limits being defined. A malicious user can consume more resources than intended and cause downstream impacts to other clients on the same hardware, eventually causing the physical server to stop responding. Users should upgrade to `1.4.4` to mitigate the issue. There is no non-code based workaround for impacted versions of the software. Users running customized versions of this software can manually set a PID limit for containers created. **CVE ID : CVE-2021-32699**	https://github.com/pterodactyl/wings/commit/e0078eee0a71d61573a94c75e6efcad069d78de3, https://github.com/pterodactyl/wings/security/advisories/GHSA-jj6m-r8jc-2gp7	A-PTE-WING-020721/142
Qnap					
myqnapcloud_link					

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Insecure Storage of Sensitive Information	16-Jun-21	4	Insecure storage of sensitive information has been reported to affect QNAP NAS running myQNAPcloud Link. If exploited, this vulnerability allows remote attackers to read sensitive information by accessing the unrestricted storage mechanism. This issue affects: QNAP Systems Inc. myQNAPcloud Link versions prior to 2.2.21 on QTS 4.5.3; versions prior to 2.2.21 on QuTS hero h4.5.2; versions prior to 2.2.21 on QuTScloud c4.5.4. **CVE ID : CVE-2021-28815**	https://www.qnap.com/zh-tw/security-advisory/qsa-21-26	A-QNA-MYQN-020721/143
Quassel-irc					
quassel					
Missing Encryption of Sensitive Data	17-Jun-21	4.3	Quassel through 0.13.1, when --require-ssl is enabled, launches without SSL or TLS support if a usable X.509 certificate is not found on the local system. **CVE ID : CVE-2021-34825**	https://github.com/quassel/quassel/pull/581	A-QUA-QUAS-020721/144
radykal					
fancy_product_designer					
Unrestricted Upload of File with Dangerous Type	21-Jun-21	7.5	The Fancy Product Designer WordPress plugin before 4.6.9 allows unauthenticated attackers to upload arbitrary files, resulting in remote code execution. **CVE ID : CVE-2021-24370**	https://wpscan.com/vulnerability/82c52461-1fdc-41e4-9f51-f9dd84962b38	A-RAD-FANC-020721/145
Rapid7					
nexpose					

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	16-Jun-21	4.3	Rapid7 Nexpose is vulnerable to a non-persistent cross-site scripting vulnerability affecting the Security Console's Filtered Asset Search feature. A specific search criterion and operator combination in Filtered Asset Search could have allowed a user to pass code through the provided search field. This issue affects version 6.6.80 and prior, and is fixed in 6.6.81. If your Security Console currently falls on or within this affected version range, ensure that you update your Security Console to the latest version. **CVE ID : CVE-2021-3535**	https://docs.rapid7.com/release-notes/nexpose/20210505/	A-RAP-NEXP-020721/146
reportportal					
service-api					
Improper Restriction of XML External Entity Reference	23-Jun-21	5	Report portal is an open source reporting and analysis framework. Starting from version 3.1.0 of the service-api XML parsing was introduced. Unfortunately the XML parser was not configured properly to prevent XML external entity (XXE) attacks. This allows a user to import a specifically-crafted XML file which imports external Document Type Definition (DTD) file with external entities for extraction of secrets from Report Portal service-api module or server-side	https://github.com/reportportal/service-api/pull/1392, https://github.com/reportportal/reportportal/security/advisories/GHSA-24wf-7vf2-pv59	A-REP-SERV-020721/147

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			request forgery. This will be resolved in the 5.4.0 release. **CVE ID : CVE-2021-29620**		
SAP					
netweaver_abap					
Improper Authentication	16-Jun-21	7.5	SAP NetWeaver ABAP Server and ABAP Platform, versions - 700, 701, 702, 731, 740, 750, 751, 752, 753, 754, 755, 804, does not create information about internal and external RFC user in consistent and distinguished format, which could lead to improper authentication and may be exploited by malicious users to obtain illegitimate access to the system. **CVE ID : CVE-2021-27610**	https://launchpad.support.sap.com/#/notes/3007182, https://wiki.scn.sap.com/wiki/pages/viewpage.action?pageId=578125999	A-SAP-NETW-020721/148
netweaver_as_abap					
Improper Authentication	16-Jun-21	7.5	SAP NetWeaver ABAP Server and ABAP Platform, versions - 700, 701, 702, 731, 740, 750, 751, 752, 753, 754, 755, 804, does not create information about internal and external RFC user in consistent and distinguished format, which could lead to improper authentication and may be exploited by malicious users to obtain illegitimate access to the system. **CVE ID : CVE-2021-27610**	https://launchpad.support.sap.com/#/notes/3007182, https://wiki.scn.sap.com/wiki/pages/viewpage.action?pageId=578125999	A-SAP-NETW-020721/149
Sensiolabs					
symfony					

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Improper Authentication	17-Jun-21	6.5	Symfony is a PHP framework for web and console applications and a set of reusable PHP components. A vulnerability related to firewall authentication is in Symfony starting with version 5.3.0 and prior to 5.3.2. When an application defines multiple firewalls, the token authenticated by one of the firewalls was available for all other firewalls. This could be abused when the application defines different providers for each part of the application, in such a situation, a user authenticated on a part of the application could be considered authenticated on the rest of the application. Starting in version 5.3.2, a patch ensures that the authenticated token is only available for the firewall that generates it. **CVE ID : CVE-2021-32693**	https://github.com/symfony/symfony/commit/3084764ad82f29dbb025df19978b9cbc3ab34728, https://github.com/symfony/symfony/security/advisories/GHSA-rfcf-m67m-jcrq, https://github.com/symfony/security-http/commit/6bf4c31219773a558b019ee12e54572174ff8129	A-SEN-SYMF-020721/150
Sonatype					
nexus_repository_manager					
Improper Limitation of a Pathname to a Restricted Directory ('Path Traversal')	18-Jun-21	4	Sonatype Nexus Repository Manager 3.x before 3.31.0 allows a remote authenticated attacker to get a list of blob files and read the content of a blob file (via a GET request) without having been granted access. **CVE ID : CVE-2021-34553**	https://support.sonatype.com/hc/en-us/articles/440243382837 1	A-SON-NEXU-020721/151

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
striptags_project					
striptags					
Access of Resource Using Incompatible Type ('Type Confusion')	18-Jun-21	5	The npm package "striptags" is an implementation of PHP's strip_tags in Typescript. In striptags before version 3.2.0, a type-confusion vulnerability can cause `striptags` to concatenate unsanitized strings when an array-like object is passed in as the `html` parameter. This can be abused by an attacker who can control the shape of their input, e.g. if query parameters are passed directly into the function. This can lead to a XSS. **CVE ID : CVE-2021-32696**	https://github.com/ericnorris/striptags/commit/f252a6b0819499cd65403707ebaf5cc925f2faca, https://github.com/ericnorris/striptags/security/advisories/GHSA-qxg5-2qff-p49r	A-STR-STRI-020721/152
Synology					
calendar					
Use of Hard-coded Credentials	18-Jun-21	5	Use of hard-coded credentials vulnerability in php component in Synology Calendar before 2.4.0-0761 allows remote attackers to obtain sensitive information via unspecified vectors. **CVE ID : CVE-2021-34812**	https://www.synology.com/security/advisory/Synology_SA_21_12	A-SYN-CALE-020721/153
diskstation_manager					
Use After Free	23-Jun-21	7.5	Use after free vulnerability in file transfer protocol component in Synology DiskStation Manager (DSM) before 6.2.3-25426-3 allows remote attackers to execute arbitrary code via unspecified vectors.	https://www.synology.com/security/advisory/Synology_SA_20_26	A-SYN-DISK-020721/154

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2021-27649		
Improper Neutralization of Special Elements in Output Used by a Downstream Component ('Injection')	23-Jun-21	5	Improper neutralization of special elements in output used by a downstream component ('Injection') vulnerability in Security Advisor report management component in Synology DiskStation Manager (DSM) before 6.2.3-25426-3 allows remote attackers to read arbitrary files via unspecified vectors. **CVE ID : CVE-2021-29084**	https://www.synology.com/security/advisory/Synology_SA_20_26	A-SYN-DISK-020721/155
Improper Neutralization of Special Elements in Output Used by a Downstream Component ('Injection')	23-Jun-21	5	Improper neutralization of special elements in output used by a downstream component ('Injection') vulnerability in file sharing management component in Synology DiskStation Manager (DSM) before 6.2.3-25426-3 allows remote attackers to read arbitrary files via unspecified vectors. **CVE ID : CVE-2021-29085**	https://www.synology.com/security/advisory/Synology_SA_20_26	A-SYN-DISK-020721/156
Exposure of Sensitive Information to an Unauthorized Actor	23-Jun-21	5	Exposure of sensitive information to an unauthorized actor vulnerability in webapi component in Synology DiskStation Manager (DSM) before 6.2.3-25426-3 allows remote attackers to obtain sensitive information via unspecified vectors. **CVE ID : CVE-2021-29086**	https://www.synology.com/security/advisory/Synology_SA_20_26	A-SYN-DISK-020721/157
Improper Limitation of	23-Jun-21	5	Improper limitation of a pathname to a restricted	https://www.synology.c	A-SYN-DISK-020721/158

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
a Pathname to a Restricted Directory ('Path Traversal')			directory ('Path Traversal') vulnerability in webapi component in Synology DiskStation Manager (DSM) before 6.2.3-25426-3 allows remote attackers to write arbitrary files via unspecified vectors. **CVE ID : CVE-2021-29087**	om/security/advisory/Synology_SA_20_26	
download_station					
Improper Neutralization of Special Elements used in a Command ('Command Injection')	18-Jun-21	6.5	Improper neutralization of special elements used in a command ('Command Injection') vulnerability in task management component in Synology Download Station before 3.8.16-3566 allows remote authenticated users to execute arbitrary code via unspecified vectors. **CVE ID : CVE-2021-34809**	https://www.synology.com/security/advisory/Synology_SA_21_11	A-SYN-DOWN-020721/159
Improper Privilege Management	18-Jun-21	6.5	Improper privilege management vulnerability in cgi component in Synology Download Station before 3.8.16-3566 allows remote authenticated users to execute arbitrary code via unspecified vectors. **CVE ID : CVE-2021-34810**	https://www.synology.com/security/advisory/Synology_SA_21_11	A-SYN-DOWN-020721/160
Server-Side Request Forgery (SSRF)	18-Jun-21	4	Server-Side Request Forgery (SSRF) vulnerability in task management component in Synology Download Station before 3.8.16-3566 allows remote authenticated users to access intranet resources via unspecified vectors.	https://www.synology.com/security/advisory/Synology_SA_21_11	A-SYN-DOWN-020721/161

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2021-34811		
media_server					
Server-Side Request Forgery (SSRF)	18-Jun-21	5	Server-Side Request Forgery (SSRF) vulnerability in cgi component in Synology Media Server before 1.8.3-2881 allows remote attackers to access intranet resources via unspecified vectors. **CVE ID : CVE-2021-34808**	https://www.synology.com/security/advisory/Synology_SA_21_10	A-SYN-MEDI-020721/162
Teamviewer					
teamviewer					
Uncontrolled Search Path Element	16-Jun-21	4.4	TeamViewer before 14.7.48644 on Windows loads untrusted DLLs in certain situations. **CVE ID : CVE-2021-34803**	https://community.teamviewer.com/English/discussion/111154/windows-v14-7-48644	A-TEA-TEAM-020721/163
thalesgroup					
safenet_keysecure					
Cleartext Storage of Sensitive Information	16-Jun-21	4.3	SafeNet KeySecure Management Console 8.12.0 is vulnerable to HTTP response splitting attacks. A remote attacker could exploit this vulnerability using specially-crafted URL to cause the server to return a split response, once the URL is clicked. **CVE ID : CVE-2021-28979**	https://www.thalesgroup.com/en	A-THA-SAFE-020721/164
theologeek					
manuskript					
Deserialization of	21-Jun-21	6.8	** DISPUTED ** Manuskript through 0.12.0 allows remote	N/A	A-THE-MANU-

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Untrusted Data			attackers to execute arbitrary code via a crafted settings.pickle file in a project file, because there is insecure deserialization via the pickle.load() function in settings.py. NOTE: the vendor's position is that the product is not intended for opening an untrusted project file. **CVE ID : CVE-2021-35196**		020721/165
tielabs					
jannah					
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	21-Jun-21	4.3	The Jannah WordPress theme before 5.4.4 did not properly sanitize the options JSON parameter in its tie_get_user_weather AJAX action before outputting it back in the page, leading to a Reflected Cross-Site Scripting (XSS) vulnerability. **CVE ID : CVE-2021-24364**	https://wpscan.com/vulnerability/1d53fbe5-a879-42ca-a9d3-768a80018382	A-TIE-JANN-020721/166
togatech					
tenvoy					
Improper Verification of Cryptographic Signature	16-Jun-21	7.5	tEnvoy contains the PGP, NaCl, and PBKDF2 in node.js and the browser (hashing, random, encryption, decryption, signatures, conversions), used by TogaTech.org. In versions prior to 7.0.3, the `verifyWithMessage` method of `tEnvoyNaClSigningKey` always returns `true` for any signature that has a SHA-512	https://github.com/TogaTech/tEnvoy/commit/a121b34a45e289d775c62e58841522891dee686b, https://github.com/TogaTech/tEnvoy/security/advi	A-TOG-TENV-020721/167

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			hash matching the SHA-512 hash of the message even if the signature was invalid. This issue is patched in version 7.0.3. As a workaround: In `tenvoy.js` under the `verifyWithMessage` method definition within the `tEnvoyNaClSigningKey` class, ensure that the return statement call to `this.verify` ends in `.verified`. **CVE ID : CVE-2021-32685**	sories/GHSA-7r96-8g3x-g36m	
torchbox					
wagtail					
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	17-Jun-21	3.5	Wagtail is an open source content management system built on Django. A cross-site scripting vulnerability exists in versions 2.13-2.13.1, versions 2.12-2.12.4, and versions prior to 2.11.8. When the `{% include_block %}` template tag is used to output the value of a plain-text StreamField block (`CharBlock`, `TextBlock` or a similar user-defined block derived from `FieldBlock`), and that block does not specify a template for rendering, the tag output is not properly escaped as HTML. This could allow users to insert arbitrary HTML or scripting. This vulnerability is only exploitable by users with the ability to author StreamField content (i.e.	https://github.com/wagtail/wagtail/security/advisories/GHSA-xfrw-hxr5-ghqf	A-TOR-WAGT-020721/168

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			users with 'editor' access to the Wagtail admin). Patched versions have been released as Wagtail 2.11.8 (for the LTS 2.11 branch), Wagtail 2.12.5, and Wagtail 2.13.2 (for the current 2.13 branch). As a workaround, site implementors who are unable to upgrade to a current supported version should audit their use of `{% include_block %}` to ensure it is not used to output `CharBlock` / `TextBlock` values with no associated template. Note that this only applies where `{% include_block %}` is used directly on that block (uses of `include_block` on a block _containing_ a CharBlock / TextBlock, such as a StructBlock, are unaffected). In these cases, the tag can be replaced with Django's `{{ ... }}` syntax - e.g. `{% include_block my_title_block %}` becomes `{{ my_title_block }}`. **CVE ID : CVE-2021-32681**		
Trendmicro					
interscan_web_security_virtual_appliance					
Improper Neutralization of Input During Web Page Generation ('Cross-site	17-Jun-21	3.5	Trend Micro InterScan Web Security Virtual Appliance version 6.5 was found to have a reflected cross-site scripting (XSS) vulnerability in the product's Captive	https://success.trendmicro.com/solution/000286452	A-TRE-INTE-020721/169

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Scripting')			Portal. **CVE ID : CVE-2021-31521**		
tsmuxer_project					
tsmuxer					
Out-of-bounds Write	23-Jun-21	4.3	Heap based buffer overflow in tsMuxer 2.6.16 allows attackers to cause a Denial of Service (DoS) by running the application with a crafted file. **CVE ID : CVE-2021-34067**	https://github.com/justdan96/tsMuxer/issues/424	A-TSM-TSMU-020721/170
Out-of-bounds Write	23-Jun-21	4.3	Heap based buffer overflow in tsMuxer 2.6.16 allows attackers to cause a Denial of Service (DoS) by running the application with a crafted file. **CVE ID : CVE-2021-34068**	https://github.com/justdan96/tsMuxer/issues/427	A-TSM-TSMU-020721/171
Divide By Zero	23-Jun-21	4.3	Divide-by-zero bug in tsMuxer 2.6.16 allows attackers to cause a Denial of Service (DoS) by running the application with a crafted file. **CVE ID : CVE-2021-34069**	https://github.com/justdan96/tsMuxer/issues/428	A-TSM-TSMU-020721/172
Out-of-bounds Read	23-Jun-21	4.3	Out-of-bounds Read in tsMuxer 2.6.16 allows attackers to cause a Denial of Service (DoS) by running the application with a crafted file. **CVE ID : CVE-2021-34070**	https://github.com/justdan96/tsMuxer/issues/426	A-TSM-TSMU-020721/173
Out-of-bounds Write	23-Jun-21	4.3	Heap based buffer overflow in tsMuxer 2.6.16 allows attackers to cause a Denial of Service (DoS) by running the application with a crafted file. **CVE ID : CVE-2021-34071**	https://github.com/justdan96/tsMuxer/issues/423	A-TSM-TSMU-020721/174
valine.js					
valine					

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Improper Control of Generation of Code ('Code Injection')	16-Jun-21	5	Valine 1.4.14 allows remote attackers to cause a denial of service (application outage) by supplying a ua (aka User-Agent) value that only specifies the product and version. **CVE ID : CVE-2021-34801**	N/A	A-VAL-VALI-020721/175
vfsjfilechooser2_project					
vfsjfilechooser2					
Allocation of Resources Without Limits or Throttling	21-Jun-21	5	A Regular Expression Denial of Service (ReDOS) vulnerability was discovered in Vfsjfilechooser2 version 0.2.9 and below which occurs when the application attempts to validate crafted URIs. **CVE ID : CVE-2021-29061**	https://github.com/yetingli/SaveResults/blob/main/md/vfsjfilechooser2.md, https://github.com/fracpete/vfsjfilechooser2/commit/9c9f2c317f3de5ece60a3ae28c371e9796e3909b, https://github.com/yetingli/PoCs/blob/main/CVE-2021-29061/Vfsjfilechooser2.md	A-VFS-VFSJ-020721/176
Vmware					
app_volumes					
Improper Input Validation	23-Jun-21	7.2	VMware Tools for Windows (11.x.y prior to 11.2.6), VMware Remote Console for Windows (12.x prior to 12.0.1) , VMware App	https://www.vmware.com/security/advisories/VMSA-2021-	A-VMW-APP_-020721/177

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Volumes (2.x prior to 2.18.10 and 4 prior to 2103) contain a local privilege escalation vulnerability. An attacker with normal access to a virtual machine may exploit this issue by placing a malicious file renamed as `openssl.cnf' in an unrestricted directory which would allow code to be executed with elevated privileges. **CVE ID : CVE-2021-21999**	0013.html	
carbon_black_app_control					
Improper Authentication	23-Jun-21	7.5	VMware Carbon Black App Control 8.0, 8.1, 8.5 prior to 8.5.8, and 8.6 prior to 8.6.2 has an authentication bypass. A malicious actor with network access to the VMware Carbon Black App Control management server might be able to obtain administrative access to the product without the need to authenticate. **CVE ID : CVE-2021-21998**	https://www.vmware.com/security/advisories/VMSA-2021-0012.html?	A-VMW-CARB-020721/178
remote_console					
Improper Input Validation	23-Jun-21	7.2	VMware Tools for Windows (11.x.y prior to 11.2.6), VMware Remote Console for Windows (12.x prior to 12.0.1) , VMware App Volumes (2.x prior to 2.18.10 and 4 prior to 2103) contain a local privilege escalation vulnerability. An attacker with normal access to a	https://www.vmware.com/security/advisories/VMSA-2021-0013.html	A-VMW-REMO-020721/179

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			virtual machine may exploit this issue by placing a malicious file renamed as `openssl.cnf' in an unrestricted directory which would allow code to be executed with elevated privileges. **CVE ID : CVE-2021-21999**		
tools					
N/A	18-Jun-21	4.9	VMware Tools for Windows (11.x.y prior to 11.3.0) contains a denial-of-service vulnerability in the VM3DMP driver. A malicious actor with local user privileges in the Windows guest operating system, where VMware Tools is installed, can trigger a PANIC in the VM3DMP driver leading to a denial-of-service condition in the Windows guest operating system. **CVE ID : CVE-2021-21997**	https://www.vmware.com/security/advisories/VMSA-2021-0011.html	A-VMW-TOOL-020721/180
Improper Input Validation	23-Jun-21	7.2	VMware Tools for Windows (11.x.y prior to 11.2.6), VMware Remote Console for Windows (12.x prior to 12.0.1) , VMware App Volumes (2.x prior to 2.18.10 and 4 prior to 2103) contain a local privilege escalation vulnerability. An attacker with normal access to a virtual machine may exploit this issue by placing a malicious file renamed as `openssl.cnf' in an unrestricted directory which	https://www.vmware.com/security/advisories/VMSA-2021-0013.html	A-VMW-TOOL-020721/181

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			would allow code to be executed with elevated privileges. **CVE ID : CVE-2021-21999**		
Wibu					
codemeter					
Out-of-bounds Read	16-Jun-21	6.4	A buffer over-read vulnerability exists in Wibu-Systems CodeMeter versions < 7.21a. An unauthenticated remote attacker can exploit this issue to disclose heap memory contents or crash the CodeMeter Runtime Server. **CVE ID : CVE-2021-20093**	https://cdn.wibu.com/fileadmin/wibu_downloads/security_advisories/Advisory_WIBU-210423-01.pdf, https://www.tenable.com/security/research/tra-2021-24	A-WIB-CODE-020721/182
Out-of-bounds Read	16-Jun-21	5	A denial of service vulnerability exists in Wibu-Systems CodeMeter versions < 7.21a. An unauthenticated remote attacker can exploit this issue to crash the CodeMeter Runtime Server. **CVE ID : CVE-2021-20094**	https://cdn.wibu.com/fileadmin/wibu_downloads/security_advisories/Advisory_WIBU-210423-02.pdf, https://www.tenable.com/security/research/tra-2021-24	A-WIB-CODE-020721/183
wphappycoders					
comments_like_dislike					
Incorrect Authorizatio	21-Jun-21	5	The Comments Like Dislike WordPress plugin before	https://wpscan.com/vuln	A-WPH-COMM-

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
n			1.1.4 allows users to like/dislike posted comments, however does not prevent them from replaying the AJAX request to add a like. This allows any user (even unauthenticated) to add unlimited like/dislike to any comment. The plugin appears to have some Restriction modes, such as Cookie Restriction, IP Restrictions, Logged In User Restriction, however, they do not prevent such attack as they only check client side **CVE ID : CVE-2021-24379**	erability/aae7a889-195c-45a3-bbe4-e6d4cd2d7fd9	020721/184
wp_config_file_editor_project					
wp_config_file_editor					
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	21-Jun-21	3.5	The WP Config File Editor WordPress plugin through 1.7.1 was affected by an Authenticated Stored Cross-Site Scripting (XSS) vulnerability. **CVE ID : CVE-2021-24367**	https://wpscan.com/vulnerability/f35b7c8f-cfb6-42b6-8a3a-8c07cd1e9da0	A-WP_-WP_C-020721/185
zettlr					
zettlr					
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	18-Jun-21	4.3	No filtering of cross-site scripting (XSS) payloads in the markdown-editor in Zettlr 1.8.7 allows attackers to perform remote code execution via a crafted file. **CVE ID : CVE-2021-26835**	https://github.com/Zettlr/Zettlr/issues/1716	A-ZET-ZETT-020721/186
znote					

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
znote					
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	18-Jun-21	3.5	A cross-site scripting (XSS) vulnerability exists in Znote 0.5.2. An attacker can insert payloads, and the code execution will happen immediately on markdown view mode. **CVE ID : CVE-2021-26834**	N/A	A-ZNO-ZNOT-020721/187
Zohocorp					
manageengine_password_manager_pro					
Insufficiently Protected Credentials	16-Jun-21	4.3	In Zoho ManageEngine Password Manager Pro before 11.1 build 11104, attackers are able to retrieve credentials via a browser extension for non-website resource types. **CVE ID : CVE-2021-31857**	https://www.manageengine.com, https://www.manageengine.com/products/passwordmanagerpro/release-notes.html#pmp11104	A-ZOH-MANA-020721/188
Zoll					
defibrillator_dashboard					
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	16-Jun-21	3.5	ZOLL Defibrillator Dashboard, v prior to 2.2,The affected product's web application could allow a low privilege user to inject parameters to contain malicious scripts to be executed by higher privilege users. **CVE ID : CVE-2021-27479**	N/A	A-ZOL-DEFI-020721/189
Use of Hard-coded	16-Jun-21	2.1	ZOLL Defibrillator Dashboard, v prior to 2.2, The affected products utilize an	N/A	A-ZOL-DEFI-020721/190

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Credentials			encryption key in the data exchange process, which is hardcoded. This could allow an attacker to gain access to sensitive information. **CVE ID : CVE-2021-27481**		
Improper Privilege Management	16-Jun-21	4.6	ZOLL Defibrillator Dashboard, v prior to 2.2,The affected products contain insecure filesystem permissions that could allow a lower privilege user to escalate privileges to an administrative level user. **CVE ID : CVE-2021-27483**	N/A	A-ZOL-DEFI-020721/191
Storing Passwords in a Recoverable Format	16-Jun-21	5	ZOLL Defibrillator Dashboard, v prior to 2.2,The application allows users to store their passwords in a recoverable format, which could allow an attacker to retrieve the credentials from the web browser. **CVE ID : CVE-2021-27485**	N/A	A-ZOL-DEFI-020721/192
Cleartext Storage of Sensitive Information	16-Jun-21	2.1	ZOLL Defibrillator Dashboard, v prior to 2.2, The affected products contain credentials stored in plaintext. This could allow an attacker to gain access to sensitive information. **CVE ID : CVE-2021-27487**	N/A	A-ZOL-DEFI-020721/193
Unrestricted Upload of File with Dangerous Type	16-Jun-21	6.5	ZOLL Defibrillator Dashboard, v prior to 2.2, The web application allows a non-administrative user to upload a malicious file. This file could allow an attacker to remotely	N/A	A-ZOL-DEFI-020721/194

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			execute arbitrary commands. **CVE ID : CVE-2021-27489**		
Hardware					
bosch					
b426					
N/A	18-Jun-21	6.8	This vulnerability could allow an attacker to hijack a session while a user is logged in the configuration web page. This vulnerability was discovered by a security researcher in B426 and found during internal product tests in B426-CN/B429-CN, and B426-M and has been fixed already starting from version 3.08 on, which was released on June 2019. **CVE ID : CVE-2021-23845**	https://psirt.bosch.com/security-advisories/bosch-sa-196933-bt.html	H-BOS-B426-020721/195
Cleartext Transmission of Sensitive Information	18-Jun-21	4.3	When using http protocol, the user password is transmitted as a clear text parameter for which it is possible to be obtained by an attacker through a MITM attack. This will be fixed starting from Firmware version 3.11.5, which will be released on the 30th of June, 2021. **CVE ID : CVE-2021-23846**	https://psirt.bosch.com/security-advisories/bosch-sa-196933-bt.html	H-BOS-B426-020721/196
b426-cn					
N/A	18-Jun-21	6.8	This vulnerability could allow an attacker to hijack a session while a user is logged in the configuration web page. This vulnerability was discovered by a security researcher in B426 and found during	https://psirt.bosch.com/security-advisories/bosch-sa-196933-bt.html	H-BOS-B426-020721/197

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			internal product tests in B426-CN/B429-CN, and B426-M and has been fixed already starting from version 3.08 on, which was released on June 2019. **CVE ID : CVE-2021-23845**		
b426-m					
N/A	18-Jun-21	6.8	This vulnerability could allow an attacker to hijack a session while a user is logged in the configuration web page. This vulnerability was discovered by a security researcher in B426 and found during internal product tests in B426-CN/B429-CN, and B426-M and has been fixed already starting from version 3.08 on, which was released on June 2019. **CVE ID : CVE-2021-23845**	https://psirt.bosch.com/security-advisories/bosch-sa-196933-bt.html	H-BOS-B426-020721/198
b429-cn					
N/A	18-Jun-21	6.8	This vulnerability could allow an attacker to hijack a session while a user is logged in the configuration web page. This vulnerability was discovered by a security researcher in B426 and found during internal product tests in B426-CN/B429-CN, and B426-M and has been fixed already starting from version 3.08 on, which was released on June 2019. **CVE ID : CVE-2021-23845**	https://psirt.bosch.com/security-advisories/bosch-sa-196933-bt.html	H-BOS-B429-020721/199
Cisco					

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
sf220-24					
Improper Authentication	16-Jun-21	9	Multiple vulnerabilities in the web-based management interface of Cisco Small Business 220 Series Smart Switches could allow an attacker to do the following: Hijack a user session Execute arbitrary commands as a root user on the underlying operating system Conduct a cross-site scripting (XSS) attack Conduct an HTML injection attack For more information about these vulnerabilities, see the Details section of this advisory. **CVE ID : CVE-2021-1541**	https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-ciscosb-multivulns-Wwyb7s5E	H-CIS-SF22-020721/200
Insufficient Session Expiration	16-Jun-21	9.3	Multiple vulnerabilities in the web-based management interface of Cisco Small Business 220 Series Smart Switches could allow an attacker to do the following: Hijack a user session Execute arbitrary commands as a root user on the underlying operating system Conduct a cross-site scripting (XSS) attack Conduct an HTML injection attack For more information about these vulnerabilities, see the Details section of this advisory. **CVE ID : CVE-2021-1542**	https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-ciscosb-multivulns-Wwyb7s5E	H-CIS-SF22-020721/201
Improper Authentication	16-Jun-21	4.3	Multiple vulnerabilities in the web-based management interface of Cisco Small Business 220 Series Smart	https://tools.cisco.com/security/center/content/Cis	H-CIS-SF22-020721/202

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Switches could allow an attacker to do the following: Hijack a user session Execute arbitrary commands as a root user on the underlying operating system Conduct a cross-site scripting (XSS) attack Conduct an HTML injection attack For more information about these vulnerabilities, see the Details section of this advisory. **CVE ID : CVE-2021-1543**	coSecurityAdvisory/cisco-sa-ciscosb-multivulns-Wwyb7s5E	
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	16-Jun-21	4.3	Multiple vulnerabilities in the web-based management interface of Cisco Small Business 220 Series Smart Switches could allow an attacker to do the following: Hijack a user session Execute arbitrary commands as a root user on the underlying operating system Conduct a cross-site scripting (XSS) attack Conduct an HTML injection attack For more information about these vulnerabilities, see the Details section of this advisory. **CVE ID : CVE-2021-1571**	https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-ciscosb-multivulns-Wwyb7s5E	H-CIS-SF22-020721/203
sf220-24p					
Improper Authentication	16-Jun-21	9	Multiple vulnerabilities in the web-based management interface of Cisco Small Business 220 Series Smart Switches could allow an attacker to do the following: Hijack a user session Execute arbitrary commands as a root	https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-ciscosb-multivulns-	H-CIS-SF22-020721/204

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			user on the underlying operating system Conduct a cross-site scripting (XSS) attack Conduct an HTML injection attack For more information about these vulnerabilities, see the Details section of this advisory. **CVE ID : CVE-2021-1541**	Wwyb7s5E	
Insufficient Session Expiration	16-Jun-21	9.3	Multiple vulnerabilities in the web-based management interface of Cisco Small Business 220 Series Smart Switches could allow an attacker to do the following: Hijack a user session Execute arbitrary commands as a root user on the underlying operating system Conduct a cross-site scripting (XSS) attack Conduct an HTML injection attack For more information about these vulnerabilities, see the Details section of this advisory. **CVE ID : CVE-2021-1542**	https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-ciscosb-multivulns-Wwyb7s5E	H-CIS-SF22-020721/205
Improper Authenticati on	16-Jun-21	4.3	Multiple vulnerabilities in the web-based management interface of Cisco Small Business 220 Series Smart Switches could allow an attacker to do the following: Hijack a user session Execute arbitrary commands as a root user on the underlying operating system Conduct a cross-site scripting (XSS) attack Conduct an HTML injection attack For more information about these	https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-ciscosb-multivulns-Wwyb7s5E	H-CIS-SF22-020721/206

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			vulnerabilities, see the Details section of this advisory. **CVE ID : CVE-2021-1543**		
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	16-Jun-21	4.3	Multiple vulnerabilities in the web-based management interface of Cisco Small Business 220 Series Smart Switches could allow an attacker to do the following: Hijack a user session Execute arbitrary commands as a root user on the underlying operating system Conduct a cross-site scripting (XSS) attack Conduct an HTML injection attack For more information about these vulnerabilities, see the Details section of this advisory. **CVE ID : CVE-2021-1571**	https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-ciscosb-multivulns-Wwyb7s5E	H-CIS-SF22-020721/207
sf220-48					
Improper Authentication	16-Jun-21	9	Multiple vulnerabilities in the web-based management interface of Cisco Small Business 220 Series Smart Switches could allow an attacker to do the following: Hijack a user session Execute arbitrary commands as a root user on the underlying operating system Conduct a cross-site scripting (XSS) attack Conduct an HTML injection attack For more information about these vulnerabilities, see the Details section of this advisory. **CVE ID : CVE-2021-1541**	https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-ciscosb-multivulns-Wwyb7s5E	H-CIS-SF22-020721/208
Insufficient	16-Jun-21	9.3	Multiple vulnerabilities in the	https://tools.	H-CIS-SF22-

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Session Expiration			web-based management interface of Cisco Small Business 220 Series Smart Switches could allow an attacker to do the following: Hijack a user session Execute arbitrary commands as a root user on the underlying operating system Conduct a cross-site scripting (XSS) attack Conduct an HTML injection attack For more information about these vulnerabilities, see the Details section of this advisory. **CVE ID : CVE-2021-1542**	cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-ciscosb-multivulns-Wwyb7s5E	020721/209
Improper Authentication	16-Jun-21	4.3	Multiple vulnerabilities in the web-based management interface of Cisco Small Business 220 Series Smart Switches could allow an attacker to do the following: Hijack a user session Execute arbitrary commands as a root user on the underlying operating system Conduct a cross-site scripting (XSS) attack Conduct an HTML injection attack For more information about these vulnerabilities, see the Details section of this advisory. **CVE ID : CVE-2021-1543**	https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-ciscosb-multivulns-Wwyb7s5E	H-CIS-SF22-020721/210
Improper Neutralization of Input During Web Page Generation ('Cross-site	16-Jun-21	4.3	Multiple vulnerabilities in the web-based management interface of Cisco Small Business 220 Series Smart Switches could allow an attacker to do the following: Hijack a user session Execute	https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-ciscosb-	H-CIS-SF22-020721/211

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Scripting')			arbitrary commands as a root user on the underlying operating system Conduct a cross-site scripting (XSS) attack Conduct an HTML injection attack For more information about these vulnerabilities, see the Details section of this advisory. **CVE ID : CVE-2021-1571**	multivulns-Wwyb7s5E	
sf220-48p					
Improper Authentication	16-Jun-21	9	Multiple vulnerabilities in the web-based management interface of Cisco Small Business 220 Series Smart Switches could allow an attacker to do the following: Hijack a user session Execute arbitrary commands as a root user on the underlying operating system Conduct a cross-site scripting (XSS) attack Conduct an HTML injection attack For more information about these vulnerabilities, see the Details section of this advisory. **CVE ID : CVE-2021-1541**	https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-ciscosb-multivulns-Wwyb7s5E	H-CIS-SF22-020721/212
Insufficient Session Expiration	16-Jun-21	9.3	Multiple vulnerabilities in the web-based management interface of Cisco Small Business 220 Series Smart Switches could allow an attacker to do the following: Hijack a user session Execute arbitrary commands as a root user on the underlying operating system Conduct a cross-site scripting (XSS)	https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-ciscosb-multivulns-Wwyb7s5E	H-CIS-SF22-020721/213

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			attack Conduct an HTML injection attack For more information about these vulnerabilities, see the Details section of this advisory. **CVE ID : CVE-2021-1542**		
Improper Authentication	16-Jun-21	4.3	Multiple vulnerabilities in the web-based management interface of Cisco Small Business 220 Series Smart Switches could allow an attacker to do the following: Hijack a user session Execute arbitrary commands as a root user on the underlying operating system Conduct a cross-site scripting (XSS) attack Conduct an HTML injection attack For more information about these vulnerabilities, see the Details section of this advisory. **CVE ID : CVE-2021-1543**	https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-ciscosb-multivulns-Wwyb7s5E	H-CIS-SF22-020721/214
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	16-Jun-21	4.3	Multiple vulnerabilities in the web-based management interface of Cisco Small Business 220 Series Smart Switches could allow an attacker to do the following: Hijack a user session Execute arbitrary commands as a root user on the underlying operating system Conduct a cross-site scripting (XSS) attack Conduct an HTML injection attack For more information about these vulnerabilities, see the Details section of this advisory.	https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-ciscosb-multivulns-Wwyb7s5E	H-CIS-SF22-020721/215

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2021-1571		
sg220-26					
Improper Authentication	16-Jun-21	9	Multiple vulnerabilities in the web-based management interface of Cisco Small Business 220 Series Smart Switches could allow an attacker to do the following: Hijack a user session Execute arbitrary commands as a root user on the underlying operating system Conduct a cross-site scripting (XSS) attack Conduct an HTML injection attack For more information about these vulnerabilities, see the Details section of this advisory. **CVE ID : CVE-2021-1541**	https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-ciscosb-multivulns-Wwyb7s5E	H-CIS-SG22-020721/216
Insufficient Session Expiration	16-Jun-21	9.3	Multiple vulnerabilities in the web-based management interface of Cisco Small Business 220 Series Smart Switches could allow an attacker to do the following: Hijack a user session Execute arbitrary commands as a root user on the underlying operating system Conduct a cross-site scripting (XSS) attack Conduct an HTML injection attack For more information about these vulnerabilities, see the Details section of this advisory. **CVE ID : CVE-2021-1542**	https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-ciscosb-multivulns-Wwyb7s5E	H-CIS-SG22-020721/217
Improper Authentication	16-Jun-21	4.3	Multiple vulnerabilities in the web-based management interface of Cisco Small	https://tools.cisco.com/security/center	H-CIS-SG22-020721/218

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Business 220 Series Smart Switches could allow an attacker to do the following: Hijack a user session Execute arbitrary commands as a root user on the underlying operating system Conduct a cross-site scripting (XSS) attack Conduct an HTML injection attack For more information about these vulnerabilities, see the Details section of this advisory. **CVE ID : CVE-2021-1543**	/content/CiscoSecurityAdvisory/cisco-sa-ciscosb-multivulns-Wwyb7s5E	
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	16-Jun-21	4.3	Multiple vulnerabilities in the web-based management interface of Cisco Small Business 220 Series Smart Switches could allow an attacker to do the following: Hijack a user session Execute arbitrary commands as a root user on the underlying operating system Conduct a cross-site scripting (XSS) attack Conduct an HTML injection attack For more information about these vulnerabilities, see the Details section of this advisory. **CVE ID : CVE-2021-1571**	https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-ciscosb-multivulns-Wwyb7s5E	H-CIS-SG22-020721/219
sg220-26p					
Improper Authentication	16-Jun-21	9	Multiple vulnerabilities in the web-based management interface of Cisco Small Business 220 Series Smart Switches could allow an attacker to do the following: Hijack a user session Execute	https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-ciscosb-	H-CIS-SG22-020721/220

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			arbitrary commands as a root user on the underlying operating system Conduct a cross-site scripting (XSS) attack Conduct an HTML injection attack For more information about these vulnerabilities, see the Details section of this advisory. **CVE ID : CVE-2021-1541**	multivulns-Wwyb7s5E	
Insufficient Session Expiration	16-Jun-21	9.3	Multiple vulnerabilities in the web-based management interface of Cisco Small Business 220 Series Smart Switches could allow an attacker to do the following: Hijack a user session Execute arbitrary commands as a root user on the underlying operating system Conduct a cross-site scripting (XSS) attack Conduct an HTML injection attack For more information about these vulnerabilities, see the Details section of this advisory. **CVE ID : CVE-2021-1542**	https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-ciscosb-multivulns-Wwyb7s5E	H-CIS-SG22-020721/221
Improper Authenticati on	16-Jun-21	4.3	Multiple vulnerabilities in the web-based management interface of Cisco Small Business 220 Series Smart Switches could allow an attacker to do the following: Hijack a user session Execute arbitrary commands as a root user on the underlying operating system Conduct a cross-site scripting (XSS) attack Conduct an HTML injection attack For more	https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-ciscosb-multivulns-Wwyb7s5E	H-CIS-SG22-020721/222

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			information about these vulnerabilities, see the Details section of this advisory. **CVE ID : CVE-2021-1543**		
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	16-Jun-21	4.3	Multiple vulnerabilities in the web-based management interface of Cisco Small Business 220 Series Smart Switches could allow an attacker to do the following: Hijack a user session Execute arbitrary commands as a root user on the underlying operating system Conduct a cross-site scripting (XSS) attack Conduct an HTML injection attack For more information about these vulnerabilities, see the Details section of this advisory. **CVE ID : CVE-2021-1571**	https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-ciscosb-multivulns-Wwyb7s5E	H-CIS-SG22-020721/223
sg220-28mp					
Improper Authentication	16-Jun-21	9	Multiple vulnerabilities in the web-based management interface of Cisco Small Business 220 Series Smart Switches could allow an attacker to do the following: Hijack a user session Execute arbitrary commands as a root user on the underlying operating system Conduct a cross-site scripting (XSS) attack Conduct an HTML injection attack For more information about these vulnerabilities, see the Details section of this advisory. **CVE ID : CVE-2021-1541**	https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-ciscosb-multivulns-Wwyb7s5E	H-CIS-SG22-020721/224

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Insufficient Session Expiration	16-Jun-21	9.3	Multiple vulnerabilities in the web-based management interface of Cisco Small Business 220 Series Smart Switches could allow an attacker to do the following: Hijack a user session Execute arbitrary commands as a root user on the underlying operating system Conduct a cross-site scripting (XSS) attack Conduct an HTML injection attack For more information about these vulnerabilities, see the Details section of this advisory. **CVE ID : CVE-2021-1542**	https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-ciscosb-multivulns-Wwyb7s5E	H-CIS-SG22-020721/225
Improper Authentication	16-Jun-21	4.3	Multiple vulnerabilities in the web-based management interface of Cisco Small Business 220 Series Smart Switches could allow an attacker to do the following: Hijack a user session Execute arbitrary commands as a root user on the underlying operating system Conduct a cross-site scripting (XSS) attack Conduct an HTML injection attack For more information about these vulnerabilities, see the Details section of this advisory. **CVE ID : CVE-2021-1543**	https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-ciscosb-multivulns-Wwyb7s5E	H-CIS-SG22-020721/226
Improper Neutralization of Input During Web Page Generation	16-Jun-21	4.3	Multiple vulnerabilities in the web-based management interface of Cisco Small Business 220 Series Smart Switches could allow an attacker to do the following:	https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-	H-CIS-SG22-020721/227

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
('Cross-site Scripting')			Hijack a user session Execute arbitrary commands as a root user on the underlying operating system Conduct a cross-site scripting (XSS) attack Conduct an HTML injection attack For more information about these vulnerabilities, see the Details section of this advisory. **CVE ID : CVE-2021-1571**	sa-ciscosb-multivulns-Wwyb7s5E	
sg220-50					
Improper Authentication	16-Jun-21	9	Multiple vulnerabilities in the web-based management interface of Cisco Small Business 220 Series Smart Switches could allow an attacker to do the following: Hijack a user session Execute arbitrary commands as a root user on the underlying operating system Conduct a cross-site scripting (XSS) attack Conduct an HTML injection attack For more information about these vulnerabilities, see the Details section of this advisory. **CVE ID : CVE-2021-1541**	https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-ciscosb-multivulns-Wwyb7s5E	H-CIS-SG22-020721/228
Insufficient Session Expiration	16-Jun-21	9.3	Multiple vulnerabilities in the web-based management interface of Cisco Small Business 220 Series Smart Switches could allow an attacker to do the following: Hijack a user session Execute arbitrary commands as a root user on the underlying operating system Conduct a	https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-ciscosb-multivulns-Wwyb7s5E	H-CIS-SG22-020721/229

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			cross-site scripting (XSS) attack Conduct an HTML injection attack For more information about these vulnerabilities, see the Details section of this advisory. **CVE ID : CVE-2021-1542**		
Improper Authentication	16-Jun-21	4.3	Multiple vulnerabilities in the web-based management interface of Cisco Small Business 220 Series Smart Switches could allow an attacker to do the following: Hijack a user session Execute arbitrary commands as a root user on the underlying operating system Conduct a cross-site scripting (XSS) attack Conduct an HTML injection attack For more information about these vulnerabilities, see the Details section of this advisory. **CVE ID : CVE-2021-1543**	https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-ciscosb-multivulns-Wwyb7s5E	H-CIS-SG22-020721/230
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	16-Jun-21	4.3	Multiple vulnerabilities in the web-based management interface of Cisco Small Business 220 Series Smart Switches could allow an attacker to do the following: Hijack a user session Execute arbitrary commands as a root user on the underlying operating system Conduct a cross-site scripting (XSS) attack Conduct an HTML injection attack For more information about these vulnerabilities, see the Details section of this advisory.	https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-ciscosb-multivulns-Wwyb7s5E	H-CIS-SG22-020721/231

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2021-1571		
sg220-50p					
Improper Authentication	16-Jun-21	9	Multiple vulnerabilities in the web-based management interface of Cisco Small Business 220 Series Smart Switches could allow an attacker to do the following: Hijack a user session Execute arbitrary commands as a root user on the underlying operating system Conduct a cross-site scripting (XSS) attack Conduct an HTML injection attack For more information about these vulnerabilities, see the Details section of this advisory. **CVE ID : CVE-2021-1541**	https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-ciscosb-multivulns-Wwyb7s5E	H-CIS-SG22-020721/232
Insufficient Session Expiration	16-Jun-21	9.3	Multiple vulnerabilities in the web-based management interface of Cisco Small Business 220 Series Smart Switches could allow an attacker to do the following: Hijack a user session Execute arbitrary commands as a root user on the underlying operating system Conduct a cross-site scripting (XSS) attack Conduct an HTML injection attack For more information about these vulnerabilities, see the Details section of this advisory. **CVE ID : CVE-2021-1542**	https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-ciscosb-multivulns-Wwyb7s5E	H-CIS-SG22-020721/233
Improper Authentication	16-Jun-21	4.3	Multiple vulnerabilities in the web-based management interface of Cisco Small	https://tools.cisco.com/security/center	H-CIS-SG22-020721/234

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Business 220 Series Smart Switches could allow an attacker to do the following: Hijack a user session Execute arbitrary commands as a root user on the underlying operating system Conduct a cross-site scripting (XSS) attack Conduct an HTML injection attack For more information about these vulnerabilities, see the Details section of this advisory. **CVE ID : CVE-2021-1543**	/content/CiscoSecurityAdvisory/cisco-sa-ciscosb-multivulns-Wwyb7s5E	
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	16-Jun-21	4.3	Multiple vulnerabilities in the web-based management interface of Cisco Small Business 220 Series Smart Switches could allow an attacker to do the following: Hijack a user session Execute arbitrary commands as a root user on the underlying operating system Conduct a cross-site scripting (XSS) attack Conduct an HTML injection attack For more information about these vulnerabilities, see the Details section of this advisory. **CVE ID : CVE-2021-1571**	https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-ciscosb-multivulns-Wwyb7s5E	H-CIS-SG22-020721/235
Dlink					
dir-2640-us					
Out-of-bounds Write	16-Jun-21	3.6	D-Link DIR-2640-US 1.01B04 is vulnerable to Buffer Overflow. There are multiple out-of-bounds vulnerabilities in some processes of D-Link AC2600(DIR-2640). Local	https://www.dlink.com/en/security-bulletin/	H-DLI-DIR--020721/236

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			ordinary users can overwrite the global variables in the .bss section, causing the process crashes or changes. **CVE ID : CVE-2021-34201**		
Out-of-bounds Write	16-Jun-21	7.2	There are multiple out-of-bounds vulnerabilities in some processes of D-Link AC2600(DIR-2640) 1.01B04. Ordinary permissions can be elevated to administrator permissions, resulting in local arbitrary code execution. An attacker can combine other vulnerabilities to further achieve the purpose of remote code execution. **CVE ID : CVE-2021-34202**	https://www.dlink.com/en/security-bulletin/, http://d-link.com	H-DLI-DIR--020721/237
Incorrect Authorization	16-Jun-21	4.8	D-Link DIR-2640-US 1.01B04 is vulnerable to Incorrect Access Control. Router ac2600 (dir-2640-us), when setting PPPoE, will start quagga process in the way of whole network monitoring, and this function uses the original default password and port. An attacker can easily use telnet to log in, modify routing information, monitor the traffic of all devices under the router, hijack DNS and phishing attacks. In addition, this interface is likely to be questioned by customers as a backdoor, because the interface should not be exposed. **CVE ID : CVE-2021-34203**	https://www.dlink.com/en/security-bulletin/, http://d-link.com	H-DLI-DIR--020721/238

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Insufficiently Protected Credentials	16-Jun-21	7.2	D-Link DIR-2640-US 1.01B04 is affected by Insufficiently Protected Credentials. D-Link AC2600(DIR-2640) stores the device system account password in plain text. It does not use linux user management. In addition, the passwords of all devices are the same, and they cannot be modified by normal users. An attacker can easily log in to the target router through the serial port and obtain root privileges. **CVE ID : CVE-2021-34204**	https://www.dlink.com/en/security-bulletin/	H-DLI-DIR--020721/239
GE					
rpv311					
Use of Hard-coded Credentials	16-Jun-21	7.5	This vulnerability allows remote attackers to execute arbitrary code on affected installations of GE Reason RPV311 14A03. Authentication is not required to exploit this vulnerability. The specific flaw exists within the firmware and filesystem of the device. The firmware and filesystem contain hard-coded default credentials. An attacker can leverage this vulnerability to execute code in the context of the download user. Was ZDI-CAN-11852. **CVE ID : CVE-2021-31477**	https://www.gegridsolutions.com/products/support/GES-2021-005%20-%20RPV311%20Security%20Notice.pdf	H-GE-RPV3-020721/240
Huawei					

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
e3372					
Improper Preservation of Permissions	22-Jun-21	4.4	Huawei LTE USB Dongle products have an improper permission assignment vulnerability. An attacker can locally access and log in to a PC to induce a user to install a specially crafted application. After successfully exploiting this vulnerability, the attacker can perform unauthenticated operations. Affected product versions include:E3372 E3372h-153TCPU-V200R002B333D01SP00C00. **CVE ID : CVE-2021-22382**	https://www.huawei.com/en/psirt/security-advisories/huawei-sa-20210602-01-permission-en	H-HUA-E337-020721/241
e8372					
Improper Preservation of Permissions	22-Jun-21	4.4	Huawei LTE USB Dongle products have an improper permission assignment vulnerability. An attacker can locally access and log in to a PC to induce a user to install a specially crafted application. After successfully exploiting this vulnerability, the attacker can perform unauthenticated operations. Affected product versions include:E3372 E3372h-153TCPU-V200R002B333D01SP00C00. **CVE ID : CVE-2021-22382**	https://www.huawei.com/en/psirt/security-advisories/huawei-sa-20210602-01-permission-en	H-HUA-E837-020721/242
ecns280					
Incorrect Authorization	22-Jun-21	4.6	There is an improper authorization vulnerability in eCNS280 V100R005C00, V100R005C10 and eSE620X	https://www.huawei.com/en/psirt/security-	H-HUA-ECNS-020721/243

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			vESS V100R001C10SPC200, V100R001C20SPC200. A file access is not authorized correctly. Attacker with low access may launch privilege escalation in a specific scenario. This may compromise the normal service. **CVE ID : CVE-2021-22361**	advisories/huawei-sa-20210519-02-cgp-en	
ecns280_td					
Allocation of Resources Without Limits or Throttling	22-Jun-21	5	There is a resource management error vulnerability in eCNS280_TD V100R005C10SPC650. An attacker needs to perform specific operations to exploit the vulnerability on the affected device. Due to improper resource management of the function, the vulnerability can be exploited to cause service abnormal on affected devices. **CVE ID : CVE-2021-22363**	https://www.huawei.com/en/psirt/security-advisories/huawei-sa-20210609-01-resource-en	H-HUA-ECNS-020721/244
Concurrent Execution using Shared Resource with Improper Synchronization ('Race Condition')	22-Jun-21	3.5	There is a race condition vulnerability in eCNS280_TD V100R005C00 and V100R005C10. There is a timing window exists in which the database can be operated by another thread that is operating concurrently. Successful exploit may cause the affected device abnormal. **CVE ID : CVE-2021-22378**	https://www.huawei.com/en/psirt/security-advisories/huawei-sa-20210602-01-cgp-en	H-HUA-ECNS-020721/245
Out-of-bounds Read	22-Jun-21	6.8	There is an out-of-bounds read vulnerability in	https://www.huawei.co	H-HUA-ECNS-

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			eCNS280_TD V100R005C10 and eSE620X vESS V100R001C10SPC200, V100R001C20SPC200, V200R001C00SPC300. The vulnerability is due to a message-handling function that contains an out-of-bounds read vulnerability. An attacker can exploit this vulnerability by sending a specific message to the target device, which could cause a Denial of Service (DoS). **CVE ID : CVE-2021-22383**	m/en/psirt/security-advisories/huawei-sa-20210616-01-cgp-en	020721/246
ese620x_vess					
Incorrect Authorization	22-Jun-21	4.6	There is an improper authorization vulnerability in eCNS280 V100R005C00, V100R005C10 and eSE620X vESS V100R001C10SPC200, V100R001C20SPC200. A file access is not authorized correctly. Attacker with low access may launch privilege escalation in a specific scenario. This may compromise the normal service. **CVE ID : CVE-2021-22361**	https://www.huawei.com/en/psirt/security-advisories/huawei-sa-20210519-02-cgp-en	H-HUA-ESE6-020721/247
Out-of-bounds Read	22-Jun-21	2.1	There is an out of bounds read vulnerability in eSE620X vESS V100R001C10SPC200, V100R001C20SPC200, V200R001C00SPC300. A local attacker can exploit this vulnerability by sending specific message to the target device. Due to insufficient	https://www.huawei.com/en/psirt/security-advisories/huawei-sa-20210526-02-outbounds-	H-HUA-ESE6-020721/248

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			validation of internal message, successful exploit may cause the process and the service abnormal. **CVE ID : CVE-2021-22365**	en	
Out-of-bounds Read	22-Jun-21	4.9	There is an out-of-bounds read vulnerability in eSE620X vESS V100R001C10SPC200, V100R001C20SPC200, V200R001C00SPC300. The vulnerability is due to a function that handles an internal message contains an out-of-bounds read vulnerability. An attacker could crafted messages between system process, successful exploit could cause Denial of Service (DoS). **CVE ID : CVE-2021-22366**	https://www.huawei.com/en/psirt/security-advisories/huawei-sa-20210526-03-dos-en	H-HUA-ESE6-020721/249
Out-of-bounds Read	22-Jun-21	6.8	There is an out-of-bounds read vulnerability in eCNS280_TD V100R005C10 and eSE620X vESS V100R001C10SPC200, V100R001C20SPC200, V200R001C00SPC300. The vulnerability is due to a message-handling function that contains an out-of-bounds read vulnerability. An attacker can exploit this vulnerability by sending a specific message to the target device, which could cause a Denial of Service (DoS). **CVE ID : CVE-2021-22383**	https://www.huawei.com/en/psirt/security-advisories/huawei-sa-20210616-01-cgp-en	H-HUA-ESE6-020721/250
ips_module					
Improper	22-Jun-21	4	There is an information leak	https://ww	H-HUA-IPS_-

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Input Validation			vulnerability in Huawei products. A module does not deal with specific input sufficiently. High privilege attackers can exploit this vulnerability by performing some operations. This can lead to information leak. Affected product versions include: IPS Module versions V500R005C00, V500R005C10, V500R005C20; NGFW Module versions V500R005C00,V500R005C10, V500R005C20; SeMG9811 versions V500R005C00; USG9500 versions V500R001C00, V500R001C20, V500R001C30, V500R001C50, V500R001C60, V500R001C80, V500R005C00, V500R005C10, V500R005C20. **CVE ID : CVE-2021-22342**	w.huawei.com/en/psirt/security-advisories/huawei-sa-20210428-01-infomationleak-en	020721/251
ngfw_module					
Improper Input Validation	22-Jun-21	4	There is an information leak vulnerability in Huawei products. A module does not deal with specific input sufficiently. High privilege attackers can exploit this vulnerability by performing some operations. This can lead to information leak. Affected product versions include: IPS Module versions	https://www.huawei.com/en/psirt/security-advisories/huawei-sa-20210428-01-infomationleak-en	H-HUA-NGFW-020721/252

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			V500R005C00, V500R005C10, V500R005C20; NGFW Module versions V500R005C00,V500R005C10, V500R005C20; SeMG9811 versions V500R005C00; USG9500 versions V500R001C00, V500R001C20, V500R001C30, V500R001C50, V500R001C60, V500R001C80, V500R005C00, V500R005C10, V500R005C20. **CVE ID : CVE-2021-22342**		
s12700					
Improper Input Validation	22-Jun-21	6.5	There is a command injection vulnerability in S12700 V200R019C00SPC500, S2700 V200R019C00SPC500, S5700 V200R019C00SPC500, S6700 V200R019C00SPC500 and S7700 V200R019C00SPC500. A module does not verify specific input sufficiently. Attackers can exploit this vulnerability by sending malicious parameters to inject command. This can compromise normal service. **CVE ID : CVE-2021-22377**	https://www.huawei.com/en/psirt/security-advisories/huawei-sa-20210602-01-cmdinj-en	H-HUA-S127-020721/253
s2700					
Improper Input Validation	22-Jun-21	6.5	There is a command injection vulnerability in S12700 V200R019C00SPC500, S2700 V200R019C00SPC500, S5700	https://www.huawei.com/en/psirt/security-	H-HUA-S270-020721/254

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			V200R019C00SPC500, S6700 V200R019C00SPC500 and S7700 V200R019C00SPC500. A module does not verify specific input sufficiently. Attackers can exploit this vulnerability by sending malicious parameters to inject command. This can compromise normal service. **CVE ID : CVE-2021-22377**	advisories/huawei-sa-20210602-01-cmdinj-en	
s5700					
Improper Input Validation	22-Jun-21	6.5	There is a command injection vulnerability in S12700 V200R019C00SPC500, S2700 V200R019C00SPC500, S5700 V200R019C00SPC500, S6700 V200R019C00SPC500 and S7700 V200R019C00SPC500. A module does not verify specific input sufficiently. Attackers can exploit this vulnerability by sending malicious parameters to inject command. This can compromise normal service. **CVE ID : CVE-2021-22377**	https://www.huawei.com/en/psirt/security-advisories/huawei-sa-20210602-01-cmdinj-en	H-HUA-S570-020721/255
s6700					
Improper Input Validation	22-Jun-21	6.5	There is a command injection vulnerability in S12700 V200R019C00SPC500, S2700 V200R019C00SPC500, S5700 V200R019C00SPC500, S6700 V200R019C00SPC500 and S7700 V200R019C00SPC500. A module does not verify specific input sufficiently. Attackers can exploit this vulnerability by sending	https://www.huawei.com/en/psirt/security-advisories/huawei-sa-20210602-01-cmdinj-en	H-HUA-S670-020721/256

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			malicious parameters to inject command. This can compromise normal service. **CVE ID : CVE-2021-22377**		
s7700					
Improper Input Validation	22-Jun-21	6.5	There is a command injection vulnerability in S12700 V200R019C00SPC500, S2700 V200R019C00SPC500, S5700 V200R019C00SPC500, S6700 V200R019C00SPC500 and S7700 V200R019C00SPC500. A module does not verify specific input sufficiently. Attackers can exploit this vulnerability by sending malicious parameters to inject command. This can compromise normal service. **CVE ID : CVE-2021-22377**	https://www.huawei.com/en/psirt/security-advisories/huawei-sa-20210602-01-cmdinj-en	H-HUA-S770-020721/257
semg9811					
Improper Input Validation	22-Jun-21	4	There is an information leak vulnerability in Huawei products. A module does not deal with specific input sufficiently. High privilege attackers can exploit this vulnerability by performing some operations. This can lead to information leak. Affected product versions include: IPS Module versions V500R005C00, V500R005C10, V500R005C20; NGFW Module versions V500R005C00,V500R005C10, V500R005C20; SeMG9811 versions V500R005C00;	https://www.huawei.com/en/psirt/security-advisories/huawei-sa-20210428-01-infomationleak-en	H-HUA-SEMG-020721/258

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			USG9500 versions V500R001C00, V500R001C20, V500R001C30, V500R001C50, V500R001C60, V500R001C80, V500R005C00, V500R005C10, V500R005C20. **CVE ID : CVE-2021-22342**		
usg9500					
Improper Input Validation	22-Jun-21	4	There is an information leak vulnerability in Huawei products. A module does not deal with specific input sufficiently. High privilege attackers can exploit this vulnerability by performing some operations. This can lead to information leak. Affected product versions include: IPS Module versions V500R005C00, V500R005C10, V500R005C20; NGFW Module versions V500R005C00,V500R005C10, V500R005C20; SeMG9811 versions V500R005C00; USG9500 versions V500R001C00, V500R001C20, V500R001C30, V500R001C50, V500R001C60, V500R001C80, V500R005C00, V500R005C10, V500R005C20.	https://www.huawei.com/en/psirt/security-advisories/huawei-sa-20210428-01-infomationleak-en	H-HUA-USG9-020721/259

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2021-22342		
Moxa					
mgate_mb3180					
Uncontrolled Resource Consumption	18-Jun-21	5	An issue was discovered on MOXA Mgate MB3180 Version 2.1 Build 18113012. Attacker could send a huge amount of TCP SYN packet to make web service's resource exhausted. Then the web server is denial-of-service. **CVE ID : CVE-2021-33823**	https://www.moxa.com/en/products/industrial-edge-connectivity/protocol-gateways/modbus-tcp-gateways/mgate-mb3180-mb3280-mb3480-series	H-MOX-MGAT-020721/260
Uncontrolled Resource Consumption	18-Jun-21	5	An issue was discovered on MOXA Mgate MB3180 Version 2.1 Build 18113012. Attackers can use slowhttptest tool to send incomplete HTTP request, which could make server keep waiting for the packet to finish the connection, until its resource exhausted. Then the web server is denial-of-service. **CVE ID : CVE-2021-33824**	https://www.moxa.com/en/products/industrial-edge-connectivity/protocol-gateways/modbus-tcp-gateways/mgate-mb3180-mb3280-mb3480-series	H-MOX-MGAT-020721/261
Nvidia					
jetson_agx_xavier_16gb					
Integer Overflow or Wraparound	22-Jun-21	4.6	Trusty (the trusted OS produced by NVIDIA for Jetson devices) driver contains a vulnerability in the	https://nvidia.custhelp.com/app/answers/detail/a_	H-NVI-JETS-020721/262

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			NVIDIA OTE protocol message parsing code where an integer overflow in a malloc() size calculation leads to a buffer overflow on the heap, which might result in information disclosure, escalation of privileges, and denial of service. **CVE ID : CVE-2021-34372**	id/5205	
Out-of-bounds Write	21-Jun-21	4.6	Bootloader contains a vulnerability in NVIDIA MB2 where a potential heap overflow might allow an attacker to control all the RAM after the heap block, leading to denial of service or code execution. **CVE ID : CVE-2021-34388**	https://nvidia.custhelp.com/app/answers/detail/a_id/5205	H-NVI-JETS-020721/263
Missing Release of Memory after Effective Lifetime	21-Jun-21	2.1	Trusty contains a vulnerability in NVIDIA OTE protocol message parsing code, which is present in all the TAs. An incorrect bounds check leads to a memory leak of a portion of the heap situated after a stream buffer. **CVE ID : CVE-2021-34389**	https://nvidia.custhelp.com/app/answers/detail/a_id/5205	H-NVI-JETS-020721/264
Deserialization of Untrusted Data	22-Jun-21	2.1	Trusty contains a vulnerability in TSEC TA which deserializes the incoming messages even though the TSEC TA does not expose any command. This vulnerability might allow an attacker to exploit the deserializer to impact code execution, causing information disclosure.	https://nvidia.custhelp.com/app/answers/detail/a_id/5205	H-NVI-JETS-020721/265

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2021-34393		
Deserialization of Untrusted Data	22-Jun-21	4.6	Trusty contains a vulnerability in all TAs whose deserializer does not reject messages with multiple occurrences of the same parameter. The deserialization of untrusted data might allow an attacker to exploit the deserializer to impact code execution. **CVE ID : CVE-2021-34394**	https://nvidia.custhelp.com/app/answers/detail/a_id/5205	H-NVI-JETS-020721/266
Out-of-bounds Write	22-Jun-21	2.1	Bootloader contains a vulnerability in NVIDIA MB2, which may cause free-the-wrong-heap, which may lead to limited denial of service. **CVE ID : CVE-2021-34397**	https://nvidia.custhelp.com/app/answers/detail/a_id/5205	H-NVI-JETS-020721/267
jetson_agx_xavier_32gb					
Integer Overflow or Wraparound	22-Jun-21	4.6	Trusty (the trusted OS produced by NVIDIA for Jetson devices) driver contains a vulnerability in the NVIDIA OTE protocol message parsing code where an integer overflow in a malloc() size calculation leads to a buffer overflow on the heap, which might result in information disclosure, escalation of privileges, and denial of service. **CVE ID : CVE-2021-34372**	https://nvidia.custhelp.com/app/answers/detail/a_id/5205	H-NVI-JETS-020721/268
Out-of-bounds Write	21-Jun-21	4.6	Bootloader contains a vulnerability in NVIDIA MB2 where a potential heap overflow might allow an attacker to control all the	https://nvidia.custhelp.com/app/answers/detail/a_id/5205	H-NVI-JETS-020721/269

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			RAM after the heap block, leading to denial of service or code execution. **CVE ID : CVE-2021-34388**		
Missing Release of Memory after Effective Lifetime	21-Jun-21	2.1	Trusty contains a vulnerability in NVIDIA OTE protocol message parsing code, which is present in all the TAs. An incorrect bounds check leads to a memory leak of a portion of the heap situated after a stream buffer. **CVE ID : CVE-2021-34389**	https://nvidia.custhelp.com/app/answers/detail/a_id/5205	H-NVI-JETS-020721/270
Deserialization of Untrusted Data	22-Jun-21	2.1	Trusty contains a vulnerability in TSEC TA which deserializes the incoming messages even though the TSEC TA does not expose any command. This vulnerability might allow an attacker to exploit the deserializer to impact code execution, causing information disclosure. **CVE ID : CVE-2021-34393**	https://nvidia.custhelp.com/app/answers/detail/a_id/5205	H-NVI-JETS-020721/271
Deserialization of Untrusted Data	22-Jun-21	4.6	Trusty contains a vulnerability in all TAs whose deserializer does not reject messages with multiple occurrences of the same parameter. The deserialization of untrusted data might allow an attacker to exploit the deserializer to impact code execution. **CVE ID : CVE-2021-34394**	https://nvidia.custhelp.com/app/answers/detail/a_id/5205	H-NVI-JETS-020721/272
Out-of-bounds	22-Jun-21	2.1	Bootloader contains a vulnerability in NVIDIA MB2, which may cause free-the-	https://nvidia.custhelp.com/app/answ	H-NVI-JETS-020721/273

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Write			wrong-heap, which may lead to limited denial of service. **CVE ID : CVE-2021-34397**	ers/detail/a_id/5205	
jetson_agx_xavier_8gb					
Integer Overflow or Wraparound	22-Jun-21	4.6	Trusty (the trusted OS produced by NVIDIA for Jetson devices) driver contains a vulnerability in the NVIDIA OTE protocol message parsing code where an integer overflow in a malloc() size calculation leads to a buffer overflow on the heap, which might result in information disclosure, escalation of privileges, and denial of service. **CVE ID : CVE-2021-34372**	https://nvidia.custhelp.com/app/answers/detail/a_id/5205	H-NVI-JETS-020721/274
Out-of-bounds Write	21-Jun-21	4.6	Bootloader contains a vulnerability in NVIDIA MB2 where a potential heap overflow might allow an attacker to control all the RAM after the heap block, leading to denial of service or code execution. **CVE ID : CVE-2021-34388**	https://nvidia.custhelp.com/app/answers/detail/a_id/5205	H-NVI-JETS-020721/275
Missing Release of Memory after Effective Lifetime	21-Jun-21	2.1	Trusty contains a vulnerability in NVIDIA OTE protocol message parsing code, which is present in all the TAs. An incorrect bounds check leads to a memory leak of a portion of the heap situated after a stream buffer. **CVE ID : CVE-2021-34389**	https://nvidia.custhelp.com/app/answers/detail/a_id/5205	H-NVI-JETS-020721/276
Deserialization of	22-Jun-21	2.1	Trusty contains a vulnerability in TSEC TA	https://nvidia.custhelp.co	H-NVI-JETS-020721/277

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Untrusted Data			which deserializes the incoming messages even though the TSEC TA does not expose any command. This vulnerability might allow an attacker to exploit the deserializer to impact code execution, causing information disclosure. **CVE ID : CVE-2021-34393**	m/app/answers/detail/a_id/5205	
Deserialization of Untrusted Data	22-Jun-21	4.6	Trusty contains a vulnerability in all TAs whose deserializer does not reject messages with multiple occurrences of the same parameter. The deserialization of untrusted data might allow an attacker to exploit the deserializer to impact code execution. **CVE ID : CVE-2021-34394**	https://nvidia.custhelp.com/app/answers/detail/a_id/5205	H-NVI-JETS-020721/278
Out-of-bounds Write	22-Jun-21	2.1	Bootloader contains a vulnerability in NVIDIA MB2, which may cause free-the-wrong-heap, which may lead to limited denial of service. **CVE ID : CVE-2021-34397**	https://nvidia.custhelp.com/app/answers/detail/a_id/5205	H-NVI-JETS-020721/279
jetson_nano					
Integer Overflow or Wraparound	22-Jun-21	4.6	Trusty (the trusted OS produced by NVIDIA for Jetson devices) driver contains a vulnerability in the NVIDIA OTE protocol message parsing code where an integer overflow in a malloc() size calculation leads to a buffer overflow on the heap, which might result in information disclosure,	https://nvidia.custhelp.com/app/answers/detail/a_id/5205	H-NVI-JETS-020721/280

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			escalation of privileges, and denial of service. **CVE ID : CVE-2021-34372**		
Out-of-bounds Write	21-Jun-21	4.6	Bootloader contains a vulnerability in NVIDIA MB2 where a potential heap overflow might allow an attacker to control all the RAM after the heap block, leading to denial of service or code execution. **CVE ID : CVE-2021-34388**	https://nvidia.custhelp.com/app/answers/detail/a_id/5205	H-NVI-JETS-020721/281
jetson_nano_2gb					
Integer Overflow or Wraparound	22-Jun-21	4.6	Trusty (the trusted OS produced by NVIDIA for Jetson devices) driver contains a vulnerability in the NVIDIA OTE protocol message parsing code where an integer overflow in a malloc() size calculation leads to a buffer overflow on the heap, which might result in information disclosure, escalation of privileges, and denial of service. **CVE ID : CVE-2021-34372**	https://nvidia.custhelp.com/app/answers/detail/a_id/5205	H-NVI-JETS-020721/282
Out-of-bounds Write	21-Jun-21	4.6	Bootloader contains a vulnerability in NVIDIA MB2 where a potential heap overflow might allow an attacker to control all the RAM after the heap block, leading to denial of service or code execution. **CVE ID : CVE-2021-34388**	https://nvidia.custhelp.com/app/answers/detail/a_id/5205	H-NVI-JETS-020721/283
jetson_tx1					
Integer	22-Jun-21	4.6	Trusty (the trusted OS	https://nvidi	H-NVI-JETS-

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Overflow or Wraparound			produced by NVIDIA for Jetson devices) driver contains a vulnerability in the NVIDIA OTE protocol message parsing code where an integer overflow in a malloc() size calculation leads to a buffer overflow on the heap, which might result in information disclosure, escalation of privileges, and denial of service. **CVE ID : CVE-2021-34372**	a.custhelp.com/app/answers/detail/a_id/5205	020721/284
Integer Overflow or Wraparound	21-Jun-21	4.6	Trusty TLK contains a vulnerability in the NVIDIA TLK kernel where an integer overflow in the calloc size calculation can cause the multiplication of count and size can overflow, which might lead to heap overflows. **CVE ID : CVE-2021-34386**	https://nvidia.custhelp.com/app/answers/detail/a_id/5205	H-NVI-JETS-020721/285
Incorrect Default Permissions	21-Jun-21	7.2	The ARM TrustZone Technology on which Trusty is based on contains a vulnerability in access permission settings where the portion of the DRAM reserved for TrustZone is identity-mapped by TLK with read, write, and execute permissions, which gives write access to kernel code and data that is otherwise mapped read only. **CVE ID : CVE-2021-34387**	https://nvidia.custhelp.com/app/answers/detail/a_id/5205	H-NVI-JETS-020721/286
Out-of-bounds Write	21-Jun-21	4.6	Bootloader contains a vulnerability in NVIDIA MB2 where a potential heap	https://nvidia.custhelp.com/app/answ	H-NVI-JETS-020721/287

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			overflow might allow an attacker to control all the RAM after the heap block, leading to denial of service or code execution. **CVE ID : CVE-2021-34388**	ers/detail/a_id/5205	
Integer Overflow or Wraparound	22-Jun-21	2.1	Trusty TLK contains a vulnerability in the NVIDIA TLK kernel function where a lack of checks allows the exploitation of an integer overflow on the size parameter of the tz_map_shared_mem function. **CVE ID : CVE-2021-34390**	https://nvidia.custhelp.com/app/answers/detail/a_id/5205	H-NVI-JETS-020721/288
Integer Overflow or Wraparound	22-Jun-21	4.9	Trusty TLK contains a vulnerability in the NVIDIA TLK kernelï¿½s tz_handle_trusted_app_smc function where a lack of integer overflow checks on the req_off and param_ofs variables leads to memory corruption of critical kernel structures. **CVE ID : CVE-2021-34391**	https://nvidia.custhelp.com/app/answers/detail/a_id/5205	H-NVI-JETS-020721/289
Integer Overflow or Wraparound	22-Jun-21	2.1	Trusty TLK contains a vulnerability in the NVIDIA TLK kernel where an integer overflow in the tz_map_shared_mem function can bypass boundary checks, which might lead to denial of service. **CVE ID : CVE-2021-34392**	https://nvidia.custhelp.com/app/answers/detail/a_id/5205	H-NVI-JETS-020721/290
Deserialization of Untrusted	22-Jun-21	2.1	Trusty contains a vulnerability in TSEC TA which deserializes the	https://nvidia.custhelp.com/app/answ	H-NVI-JETS-020721/291

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Data			incoming messages even though the TSEC TA does not expose any command. This vulnerability might allow an attacker to exploit the deserializer to impact code execution, causing information disclosure. **CVE ID : CVE-2021-34393**	ers/detail/a_id/5205	
Incorrect Default Permissions	22-Jun-21	3.6	Trusty TLK contains a vulnerability in its access permission settings where it does not properly restrict access to a resource from a user with local privileges, which might lead to limited information disclosure and limited denial of service. **CVE ID : CVE-2021-34395**	https://nvidia.custhelp.com/app/answers/detail/a_id/5205	H-NVI-JETS-020721/292
jetson_tx2					
Integer Overflow or Wraparound	22-Jun-21	4.6	Trusty (the trusted OS produced by NVIDIA for Jetson devices) driver contains a vulnerability in the NVIDIA OTE protocol message parsing code where an integer overflow in a malloc() size calculation leads to a buffer overflow on the heap, which might result in information disclosure, escalation of privileges, and denial of service. **CVE ID : CVE-2021-34372**	https://nvidia.custhelp.com/app/answers/detail/a_id/5205	H-NVI-JETS-020721/293
Out-of-bounds Write	21-Jun-21	4.6	Bootloader contains a vulnerability in NVIDIA MB2 where a potential heap overflow might allow an attacker to control all the	https://nvidia.custhelp.com/app/answers/detail/a_id/5205	H-NVI-JETS-020721/294

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			RAM after the heap block, leading to denial of service or code execution. **CVE ID : CVE-2021-34388**		
Missing Release of Memory after Effective Lifetime	21-Jun-21	2.1	Trusty contains a vulnerability in NVIDIA OTE protocol message parsing code, which is present in all the TAs. An incorrect bounds check leads to a memory leak of a portion of the heap situated after a stream buffer. **CVE ID : CVE-2021-34389**	https://nvidia.custhelp.com/app/answers/detail/a_id/5205	H-NVI-JETS-020721/295
Deserialization of Untrusted Data	22-Jun-21	2.1	Trusty contains a vulnerability in TSEC TA which deserializes the incoming messages even though the TSEC TA does not expose any command. This vulnerability might allow an attacker to exploit the deserializer to impact code execution, causing information disclosure. **CVE ID : CVE-2021-34393**	https://nvidia.custhelp.com/app/answers/detail/a_id/5205	H-NVI-JETS-020721/296
Deserialization of Untrusted Data	22-Jun-21	4.6	Trusty contains a vulnerability in all TAs whose deserializer does not reject messages with multiple occurrences of the same parameter. The deserialization of untrusted data might allow an attacker to exploit the deserializer to impact code execution. **CVE ID : CVE-2021-34394**	https://nvidia.custhelp.com/app/answers/detail/a_id/5205	H-NVI-JETS-020721/297
Incorrect Authorizatio	22-Jun-21	2.1	Bootloader contains a vulnerability in access permission settings where	https://nvidia.custhelp.com/app/answ	H-NVI-JETS-020721/298

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
n			unauthorized software may be able to overwrite NVIDIA MB2 code, which would result in limited denial of service. **CVE ID : CVE-2021-34396**	ers/detail/a_id/5205	
Out-of-bounds Write	22-Jun-21	2.1	Bootloader contains a vulnerability in NVIDIA MB2, which may cause free-the-wrong-heap, which may lead to limited denial of service. **CVE ID : CVE-2021-34397**	https://nvidia.custhelp.com/app/answers/detail/a_id/5205	H-NVI-JETS-020721/299
jetson_tx2i					
Integer Overflow or Wraparound	22-Jun-21	4.6	Trusty (the trusted OS produced by NVIDIA for Jetson devices) driver contains a vulnerability in the NVIDIA OTE protocol message parsing code where an integer overflow in a malloc() size calculation leads to a buffer overflow on the heap, which might result in information disclosure, escalation of privileges, and denial of service. **CVE ID : CVE-2021-34372**	https://nvidia.custhelp.com/app/answers/detail/a_id/5205	H-NVI-JETS-020721/300
Out-of-bounds Write	21-Jun-21	4.6	Bootloader contains a vulnerability in NVIDIA MB2 where a potential heap overflow might allow an attacker to control all the RAM after the heap block, leading to denial of service or code execution. **CVE ID : CVE-2021-34388**	https://nvidia.custhelp.com/app/answers/detail/a_id/5205	H-NVI-JETS-020721/301
Missing Release of	21-Jun-21	2.1	Trusty contains a vulnerability in NVIDIA OTE	https://nvidia.custhelp.co	H-NVI-JETS-020721/302

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Memory after Effective Lifetime			protocol message parsing code, which is present in all the TAs. An incorrect bounds check leads to a memory leak of a portion of the heap situated after a stream buffer. **CVE ID : CVE-2021-34389**	m/app/answers/detail/a_id/5205	
Deserialization of Untrusted Data	22-Jun-21	2.1	Trusty contains a vulnerability in TSEC TA which deserializes the incoming messages even though the TSEC TA does not expose any command. This vulnerability might allow an attacker to exploit the deserializer to impact code execution, causing information disclosure. **CVE ID : CVE-2021-34393**	https://nvidia.custhelp.com/app/answers/detail/a_id/5205	H-NVI-JETS-020721/303
Deserialization of Untrusted Data	22-Jun-21	4.6	Trusty contains a vulnerability in all TAs whose deserializer does not reject messages with multiple occurrences of the same parameter. The deserialization of untrusted data might allow an attacker to exploit the deserializer to impact code execution. **CVE ID : CVE-2021-34394**	https://nvidia.custhelp.com/app/answers/detail/a_id/5205	H-NVI-JETS-020721/304
Incorrect Authorization	22-Jun-21	2.1	Bootloader contains a vulnerability in access permission settings where unauthorized software may be able to overwrite NVIDIA MB2 code, which would result in limited denial of service. **CVE ID : CVE-2021-34396**	https://nvidia.custhelp.com/app/answers/detail/a_id/5205	H-NVI-JETS-020721/305

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Out-of-bounds Write	22-Jun-21	2.1	Bootloader contains a vulnerability in NVIDIA MB2, which may cause free-the-wrong-heap, which may lead to limited denial of service. **CVE ID : CVE-2021-34397**	https://nvidia.custhelp.com/app/answers/detail/a_id/5205	H-NVI-JETS-020721/306
jetson_tx2_4gb					
Integer Overflow or Wraparound	22-Jun-21	4.6	Trusty (the trusted OS produced by NVIDIA for Jetson devices) driver contains a vulnerability in the NVIDIA OTE protocol message parsing code where an integer overflow in a malloc() size calculation leads to a buffer overflow on the heap, which might result in information disclosure, escalation of privileges, and denial of service. **CVE ID : CVE-2021-34372**	https://nvidia.custhelp.com/app/answers/detail/a_id/5205	H-NVI-JETS-020721/307
Out-of-bounds Write	21-Jun-21	4.6	Bootloader contains a vulnerability in NVIDIA MB2 where a potential heap overflow might allow an attacker to control all the RAM after the heap block, leading to denial of service or code execution. **CVE ID : CVE-2021-34388**	https://nvidia.custhelp.com/app/answers/detail/a_id/5205	H-NVI-JETS-020721/308
Missing Release of Memory after Effective Lifetime	21-Jun-21	2.1	Trusty contains a vulnerability in NVIDIA OTE protocol message parsing code, which is present in all the TAs. An incorrect bounds check leads to a memory leak of a portion of the heap situated after a stream buffer.	https://nvidia.custhelp.com/app/answers/detail/a_id/5205	H-NVI-JETS-020721/309

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2021-34389		
Deserialization of Untrusted Data	22-Jun-21	2.1	Trusty contains a vulnerability in TSEC TA which deserializes the incoming messages even though the TSEC TA does not expose any command. This vulnerability might allow an attacker to exploit the deserializer to impact code execution, causing information disclosure. **CVE ID : CVE-2021-34393**	https://nvidia.custhelp.com/app/answers/detail/a_id/5205	H-NVI-JETS-020721/310
Deserialization of Untrusted Data	22-Jun-21	4.6	Trusty contains a vulnerability in all TAs whose deserializer does not reject messages with multiple occurrences of the same parameter. The deserialization of untrusted data might allow an attacker to exploit the deserializer to impact code execution. **CVE ID : CVE-2021-34394**	https://nvidia.custhelp.com/app/answers/detail/a_id/5205	H-NVI-JETS-020721/311
Incorrect Authorization	22-Jun-21	2.1	Bootloader contains a vulnerability in access permission settings where unauthorized software may be able to overwrite NVIDIA MB2 code, which would result in limited denial of service. **CVE ID : CVE-2021-34396**	https://nvidia.custhelp.com/app/answers/detail/a_id/5205	H-NVI-JETS-020721/312
Out-of-bounds Write	22-Jun-21	2.1	Bootloader contains a vulnerability in NVIDIA MB2, which may cause free-the-wrong-heap, which may lead to limited denial of service.	https://nvidia.custhelp.com/app/answers/detail/a_id/5205	H-NVI-JETS-020721/313

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2021-34397		
jetson_tx2_nx					
Integer Overflow or Wraparound	22-Jun-21	4.6	Trusty (the trusted OS produced by NVIDIA for Jetson devices) driver contains a vulnerability in the NVIDIA OTE protocol message parsing code where an integer overflow in a malloc() size calculation leads to a buffer overflow on the heap, which might result in information disclosure, escalation of privileges, and denial of service. **CVE ID : CVE-2021-34372**	https://nvidia.custhelp.com/app/answers/detail/a_id/5205	H-NVI-JETS-020721/314
Out-of-bounds Write	21-Jun-21	4.6	Bootloader contains a vulnerability in NVIDIA MB2 where a potential heap overflow might allow an attacker to control all the RAM after the heap block, leading to denial of service or code execution. **CVE ID : CVE-2021-34388**	https://nvidia.custhelp.com/app/answers/detail/a_id/5205	H-NVI-JETS-020721/315
Missing Release of Memory after Effective Lifetime	21-Jun-21	2.1	Trusty contains a vulnerability in NVIDIA OTE protocol message parsing code, which is present in all the TAs. An incorrect bounds check leads to a memory leak of a portion of the heap situated after a stream buffer. **CVE ID : CVE-2021-34389**	https://nvidia.custhelp.com/app/answers/detail/a_id/5205	H-NVI-JETS-020721/316
Deserialization of Untrusted Data	22-Jun-21	2.1	Trusty contains a vulnerability in TSEC TA which deserializes the incoming messages even	https://nvidia.custhelp.com/app/answers/detail/a_	H-NVI-JETS-020721/317

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			though the TSEC TA does not expose any command. This vulnerability might allow an attacker to exploit the deserializer to impact code execution, causing information disclosure. **CVE ID : CVE-2021-34393**	id/5205	
Deserialization of Untrusted Data	22-Jun-21	4.6	Trusty contains a vulnerability in all TAs whose deserializer does not reject messages with multiple occurrences of the same parameter. The deserialization of untrusted data might allow an attacker to exploit the deserializer to impact code execution. **CVE ID : CVE-2021-34394**	https://nvidia.custhelp.com/app/answers/detail/a_id/5205	H-NVI-JETS-020721/318
Incorrect Authorization	22-Jun-21	2.1	Bootloader contains a vulnerability in access permission settings where unauthorized software may be able to overwrite NVIDIA MB2 code, which would result in limited denial of service. **CVE ID : CVE-2021-34396**	https://nvidia.custhelp.com/app/answers/detail/a_id/5205	H-NVI-JETS-020721/319
Out-of-bounds Write	22-Jun-21	2.1	Bootloader contains a vulnerability in NVIDIA MB2, which may cause free-the-wrong-heap, which may lead to limited denial of service. **CVE ID : CVE-2021-34397**	https://nvidia.custhelp.com/app/answers/detail/a_id/5205	H-NVI-JETS-020721/320
jetson_xavier_nx					
Integer Overflow or Wraparound	22-Jun-21	4.6	Trusty (the trusted OS produced by NVIDIA for Jetson devices) driver	https://nvidia.custhelp.com/app/answ	H-NVI-JETS-020721/321

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			contains a vulnerability in the NVIDIA OTE protocol message parsing code where an integer overflow in a malloc() size calculation leads to a buffer overflow on the heap, which might result in information disclosure, escalation of privileges, and denial of service. **CVE ID : CVE-2021-34372**	ers/detail/a_id/5205	
Out-of-bounds Write	21-Jun-21	4.6	Bootloader contains a vulnerability in NVIDIA MB2 where a potential heap overflow might allow an attacker to control all the RAM after the heap block, leading to denial of service or code execution. **CVE ID : CVE-2021-34388**	https://nvidia.custhelp.com/app/answers/detail/a_id/5205	H-NVI-JETS-020721/322
Missing Release of Memory after Effective Lifetime	21-Jun-21	2.1	Trusty contains a vulnerability in NVIDIA OTE protocol message parsing code, which is present in all the TAs. An incorrect bounds check leads to a memory leak of a portion of the heap situated after a stream buffer. **CVE ID : CVE-2021-34389**	https://nvidia.custhelp.com/app/answers/detail/a_id/5205	H-NVI-JETS-020721/323
Deserialization of Untrusted Data	22-Jun-21	2.1	Trusty contains a vulnerability in TSEC TA which deserializes the incoming messages even though the TSEC TA does not expose any command. This vulnerability might allow an attacker to exploit the deserializer to impact code execution, causing	https://nvidia.custhelp.com/app/answers/detail/a_id/5205	H-NVI-JETS-020721/324

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			information disclosure. **CVE ID : CVE-2021-34393**		
Deserialization of Untrusted Data	22-Jun-21	4.6	Trusty contains a vulnerability in all TAs whose deserializer does not reject messages with multiple occurrences of the same parameter. The deserialization of untrusted data might allow an attacker to exploit the deserializer to impact code execution. **CVE ID : CVE-2021-34394**	https://nvidia.custhelp.com/app/answers/detail/a_id/5205	H-NVI-JETS-020721/325
Out-of-bounds Write	22-Jun-21	2.1	Bootloader contains a vulnerability in NVIDIA MB2, which may cause free-the-wrong-heap, which may lead to limited denial of service. **CVE ID : CVE-2021-34397**	https://nvidia.custhelp.com/app/answers/detail/a_id/5205	H-NVI-JETS-020721/326
protectimus					
slim_nfc_70					
Improper Authentication	16-Jun-21	1.9	Protectimus SLIM NFC 70 10.01 devices allow a Time Traveler attack in which attackers can predict TOTP passwords in certain situations. The time value used by the device can be set independently from the used seed value for generating time-based one-time passwords, without authentication. Thus, an attacker with short-time physical access to a device can set the internal real-time clock (RTC) to the future, generate one-time	N/A	H-PRO-SLIM-020721/327

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			passwords, and reset the clock to the current time. This allows the generation of valid future time-based one-time passwords without having further access to the hardware token. **CVE ID : CVE-2021-32033**		
sing4g					
4gee_router_hh70vb					
Uncontrolled Resource Consumption	18-Jun-21	5	An issue was discovered on 4GEE ROUTER HH70VB Version HH70_E1_02.00_22. Attackers can use slowhttptest tool to send incomplete HTTP request, which could make server keep waiting for the packet to finish the connection, until its resource exhausted. Then the web server is denial-of-service. **CVE ID : CVE-2021-33822**	https://www.sing4g.com/product-page/4gee-router-hh70vb-4g-300mbps-2lan-32wifi	H-SIN-4GEE-020721/328
Trendnet					
tw100-s4w1ca					
Cross-Site Request Forgery (CSRF)	17-Jun-21	6.8	In TrendNet TW100-S4W1CA 2.3.32, due to a lack of proper session controls, a threat actor could make unauthorized changes to an affected router via a specially crafted web page. If an authenticated user were to interact with a malicious web page it could allow for a complete takeover of the router. **CVE ID : CVE-2021-32424**	N/A	H-TRE-TW10-020721/329

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	17-Jun-21	4.3	In TrendNet TW100-S4W1CA 2.3.32, it is possible to inject arbitrary JavaScript into the router's web interface via the "echo" command. **CVE ID : CVE-2021-32426**	N/A	H-TRE-TW10-020721/330
ui					
camera_g3_flex					
Uncontrolled Resource Consumption	18-Jun-21	5	An issue was discovered in UniFi Protect G3 FLEX Camera Version UVC.v4.30.0.67. Attackers can use slowhttptest tool to send incomplete HTTP request, which could make server keep waiting for the packet to finish the connection, until its resource exhausted. Then the web server is denial-of-service. **CVE ID : CVE-2021-33818**	https://store.ui.com/collections/unifi-protect-cameras/products/unifi-video-g3-flex-camera	H-UI-CAME-020721/331
Uncontrolled Resource Consumption	18-Jun-21	5	An issue was discovered in UniFi Protect G3 FLEX Camera Version UVC.v4.30.0.67.Attacker could send a huge amount of TCP SYN packet to make web service's resource exhausted. Then the web server is denial-of-service. **CVE ID : CVE-2021-33820**	https://store.ui.com/collections/unifi-protect-cameras/products/unifi-video-g3-flex-camera	H-UI-CAME-020721/332
Operating System					
bosch					
b426-cn_firmware					
N/A	18-Jun-21	6.8	This vulnerability could allow an attacker to hijack a session	https://psirt.bosch.com/s	O-BOS-B426-

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			while a user is logged in the configuration web page. This vulnerability was discovered by a security researcher in B426 and found during internal product tests in B426-CN/B429-CN, and B426-M and has been fixed already starting from version 3.08 on, which was released on June 2019. **CVE ID : CVE-2021-23845**	ecurity-advisories/bosch-sa-196933-bt.html	020721/333
b426-m_firmware					
N/A	18-Jun-21	6.8	This vulnerability could allow an attacker to hijack a session while a user is logged in the configuration web page. This vulnerability was discovered by a security researcher in B426 and found during internal product tests in B426-CN/B429-CN, and B426-M and has been fixed already starting from version 3.08 on, which was released on June 2019. **CVE ID : CVE-2021-23845**	https://psirt.bosch.com/security-advisories/bosch-sa-196933-bt.html	O-BOS-B426-020721/334
b426_firmware					
N/A	18-Jun-21	6.8	This vulnerability could allow an attacker to hijack a session while a user is logged in the configuration web page. This vulnerability was discovered by a security researcher in B426 and found during internal product tests in B426-CN/B429-CN, and B426-M and has been fixed already starting from version	https://psirt.bosch.com/security-advisories/bosch-sa-196933-bt.html	O-BOS-B426-020721/335

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			3.08 on, which was released on June 2019. **CVE ID : CVE-2021-23845**		
Cleartext Transmission of Sensitive Information	18-Jun-21	4.3	When using http protocol, the user password is transmitted as a clear text parameter for which it is possible to be obtained by an attacker through a MITM attack. This will be fixed starting from Firmware version 3.11.5, which will be released on the 30th of June, 2021. **CVE ID : CVE-2021-23846**	https://psirt.bosch.com/security-advisories/bosch-sa-196933-bt.html	O-BOS-B426-020721/336
b429-cn_firmware					
N/A	18-Jun-21	6.8	This vulnerability could allow an attacker to hijack a session while a user is logged in the configuration web page. This vulnerability was discovered by a security researcher in B426 and found during internal product tests in B426-CN/B429-CN, and B426-M and has been fixed already starting from version 3.08 on, which was released on June 2019. **CVE ID : CVE-2021-23845**	https://psirt.bosch.com/security-advisories/bosch-sa-196933-bt.html	O-BOS-B429-020721/337
Cisco					
asyncos					
Improper Certificate Validation	16-Jun-21	5.8	A vulnerability in the Cisco Advanced Malware Protection (AMP) for Endpoints integration of Cisco AsyncOS for Cisco Email Security Appliance (ESA) and Cisco Web Security Appliance	https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-esa-wsa-	O-CIS-ASYN-020721/338

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			(WSA) could allow an unauthenticated, remote attacker to intercept traffic between an affected device and the AMP servers. This vulnerability is due to improper certificate validation when an affected device establishes TLS connections. A man-in-the-middle attacker could exploit this vulnerability by sending a crafted TLS packet to an affected device. A successful exploit could allow the attacker to spoof a trusted host and then extract sensitive information or alter certain API requests. **CVE ID : CVE-2021-1566**	cert-vali-n8L97RW	
packaged_contact_center_enterprise					
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	16-Jun-21	4.3	A vulnerability in the web-based management interface of Cisco Unified Intelligence Center could allow an unauthenticated, remote attacker to conduct a cross-site scripting (XSS) attack against a user of the interface. This vulnerability exists because the web-based management interface does not properly validate user-supplied input. An attacker could exploit this vulnerability by persuading a user of the interface to click a crafted link. A successful exploit could allow the attacker to execute arbitrary	https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-cuic-xss-csHUdtrL	O-CIS-PACK-020721/339

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			script code in the context of the interface or access sensitive, browser-based information. **CVE ID : CVE-2021-1395**		
sf220-24p_firmware					
Improper Authentication	16-Jun-21	9	Multiple vulnerabilities in the web-based management interface of Cisco Small Business 220 Series Smart Switches could allow an attacker to do the following: Hijack a user session Execute arbitrary commands as a root user on the underlying operating system Conduct a cross-site scripting (XSS) attack Conduct an HTML injection attack For more information about these vulnerabilities, see the Details section of this advisory. **CVE ID : CVE-2021-1541**	https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-ciscosb-multivulns-Wwyb7s5E	O-CIS-SF22-020721/340
Insufficient Session Expiration	16-Jun-21	9.3	Multiple vulnerabilities in the web-based management interface of Cisco Small Business 220 Series Smart Switches could allow an attacker to do the following: Hijack a user session Execute arbitrary commands as a root user on the underlying operating system Conduct a cross-site scripting (XSS) attack Conduct an HTML injection attack For more information about these vulnerabilities, see the Details section of this advisory.	https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-ciscosb-multivulns-Wwyb7s5E	O-CIS-SF22-020721/341

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2021-1542		
Improper Authentication	16-Jun-21	4.3	Multiple vulnerabilities in the web-based management interface of Cisco Small Business 220 Series Smart Switches could allow an attacker to do the following: Hijack a user session Execute arbitrary commands as a root user on the underlying operating system Conduct a cross-site scripting (XSS) attack Conduct an HTML injection attack For more information about these vulnerabilities, see the Details section of this advisory. **CVE ID : CVE-2021-1543**	https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-ciscosb-multivulns-Wwyb7s5E	O-CIS-SF22-020721/342
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	16-Jun-21	4.3	Multiple vulnerabilities in the web-based management interface of Cisco Small Business 220 Series Smart Switches could allow an attacker to do the following: Hijack a user session Execute arbitrary commands as a root user on the underlying operating system Conduct a cross-site scripting (XSS) attack Conduct an HTML injection attack For more information about these vulnerabilities, see the Details section of this advisory. **CVE ID : CVE-2021-1571**	https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-ciscosb-multivulns-Wwyb7s5E	O-CIS-SF22-020721/343
sf220-24_firmware					
Improper Authentication	16-Jun-21	9	Multiple vulnerabilities in the web-based management interface of Cisco Small	https://tools.cisco.com/security/center	O-CIS-SF22-020721/344

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Business 220 Series Smart Switches could allow an attacker to do the following: Hijack a user session Execute arbitrary commands as a root user on the underlying operating system Conduct a cross-site scripting (XSS) attack Conduct an HTML injection attack For more information about these vulnerabilities, see the Details section of this advisory. **CVE ID : CVE-2021-1541**	/content/CiscoSecurityAdvisory/cisco-sa-ciscosb-multivulns-Wwyb7s5E	
Insufficient Session Expiration	16-Jun-21	9.3	Multiple vulnerabilities in the web-based management interface of Cisco Small Business 220 Series Smart Switches could allow an attacker to do the following: Hijack a user session Execute arbitrary commands as a root user on the underlying operating system Conduct a cross-site scripting (XSS) attack Conduct an HTML injection attack For more information about these vulnerabilities, see the Details section of this advisory. **CVE ID : CVE-2021-1542**	https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-ciscosb-multivulns-Wwyb7s5E	O-CIS-SF22-020721/345
Improper Authentication	16-Jun-21	4.3	Multiple vulnerabilities in the web-based management interface of Cisco Small Business 220 Series Smart Switches could allow an attacker to do the following: Hijack a user session Execute arbitrary commands as a root user on the underlying	https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-ciscosb-multivulns-Wwyb7s5E	O-CIS-SF22-020721/346

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			operating system Conduct a cross-site scripting (XSS) attack Conduct an HTML injection attack For more information about these vulnerabilities, see the Details section of this advisory. **CVE ID : CVE-2021-1543**		
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	16-Jun-21	4.3	Multiple vulnerabilities in the web-based management interface of Cisco Small Business 220 Series Smart Switches could allow an attacker to do the following: Hijack a user session Execute arbitrary commands as a root user on the underlying operating system Conduct a cross-site scripting (XSS) attack Conduct an HTML injection attack For more information about these vulnerabilities, see the Details section of this advisory. **CVE ID : CVE-2021-1571**	https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-ciscosb-multivulns-Wwyb7s5E	O-CIS-SF22-020721/347
sf220-48p_firmware					
Improper Authentication	16-Jun-21	9	Multiple vulnerabilities in the web-based management interface of Cisco Small Business 220 Series Smart Switches could allow an attacker to do the following: Hijack a user session Execute arbitrary commands as a root user on the underlying operating system Conduct a cross-site scripting (XSS) attack Conduct an HTML injection attack For more	https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-ciscosb-multivulns-Wwyb7s5E	O-CIS-SF22-020721/348

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			information about these vulnerabilities, see the Details section of this advisory. **CVE ID : CVE-2021-1541**		
Insufficient Session Expiration	16-Jun-21	9.3	Multiple vulnerabilities in the web-based management interface of Cisco Small Business 220 Series Smart Switches could allow an attacker to do the following: Hijack a user session Execute arbitrary commands as a root user on the underlying operating system Conduct a cross-site scripting (XSS) attack Conduct an HTML injection attack For more information about these vulnerabilities, see the Details section of this advisory. **CVE ID : CVE-2021-1542**	https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-ciscosb-multivulns-Wwyb7s5E	O-CIS-SF22-020721/349
Improper Authenticati on	16-Jun-21	4.3	Multiple vulnerabilities in the web-based management interface of Cisco Small Business 220 Series Smart Switches could allow an attacker to do the following: Hijack a user session Execute arbitrary commands as a root user on the underlying operating system Conduct a cross-site scripting (XSS) attack Conduct an HTML injection attack For more information about these vulnerabilities, see the Details section of this advisory. **CVE ID : CVE-2021-1543**	https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-ciscosb-multivulns-Wwyb7s5E	O-CIS-SF22-020721/350
Improper	16-Jun-21	4.3	Multiple vulnerabilities in the	https://tools.	O-CIS-SF22-

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Neutralization of Input During Web Page Generation ('Cross-site Scripting')			web-based management interface of Cisco Small Business 220 Series Smart Switches could allow an attacker to do the following: Hijack a user session Execute arbitrary commands as a root user on the underlying operating system Conduct a cross-site scripting (XSS) attack Conduct an HTML injection attack For more information about these vulnerabilities, see the Details section of this advisory. **CVE ID : CVE-2021-1571**	cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-ciscosb-multivulns-Wwyb7s5E	020721/351
sf220-48_firmware					
Improper Authentication	16-Jun-21	9	Multiple vulnerabilities in the web-based management interface of Cisco Small Business 220 Series Smart Switches could allow an attacker to do the following: Hijack a user session Execute arbitrary commands as a root user on the underlying operating system Conduct a cross-site scripting (XSS) attack Conduct an HTML injection attack For more information about these vulnerabilities, see the Details section of this advisory. **CVE ID : CVE-2021-1541**	https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-ciscosb-multivulns-Wwyb7s5E	O-CIS-SF22-020721/352
Insufficient Session Expiration	16-Jun-21	9.3	Multiple vulnerabilities in the web-based management interface of Cisco Small Business 220 Series Smart Switches could allow an	https://tools.cisco.com/security/center/content/CiscoSecurityAd	O-CIS-SF22-020721/353

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			attacker to do the following: Hijack a user session Execute arbitrary commands as a root user on the underlying operating system Conduct a cross-site scripting (XSS) attack Conduct an HTML injection attack For more information about these vulnerabilities, see the Details section of this advisory. **CVE ID : CVE-2021-1542**	visory/cisco-sa-ciscosb-multivulns-Wwyb7s5E	
Improper Authentication	16-Jun-21	4.3	Multiple vulnerabilities in the web-based management interface of Cisco Small Business 220 Series Smart Switches could allow an attacker to do the following: Hijack a user session Execute arbitrary commands as a root user on the underlying operating system Conduct a cross-site scripting (XSS) attack Conduct an HTML injection attack For more information about these vulnerabilities, see the Details section of this advisory. **CVE ID : CVE-2021-1543**	https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-ciscosb-multivulns-Wwyb7s5E	O-CIS-SF22-020721/354
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	16-Jun-21	4.3	Multiple vulnerabilities in the web-based management interface of Cisco Small Business 220 Series Smart Switches could allow an attacker to do the following: Hijack a user session Execute arbitrary commands as a root user on the underlying operating system Conduct a cross-site scripting (XSS)	https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-ciscosb-multivulns-Wwyb7s5E	O-CIS-SF22-020721/355

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			attack Conduct an HTML injection attack For more information about these vulnerabilities, see the Details section of this advisory. **CVE ID : CVE-2021-1571**		
sg220-26p_firmware					
Improper Authenticati on	16-Jun-21	9	Multiple vulnerabilities in the web-based management interface of Cisco Small Business 220 Series Smart Switches could allow an attacker to do the following: Hijack a user session Execute arbitrary commands as a root user on the underlying operating system Conduct a cross-site scripting (XSS) attack Conduct an HTML injection attack For more information about these vulnerabilities, see the Details section of this advisory. **CVE ID : CVE-2021-1541**	https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-ciscosb-multivulns-Wwyb7s5E	O-CIS-SG22-020721/356
Insufficient Session Expiration	16-Jun-21	9.3	Multiple vulnerabilities in the web-based management interface of Cisco Small Business 220 Series Smart Switches could allow an attacker to do the following: Hijack a user session Execute arbitrary commands as a root user on the underlying operating system Conduct a cross-site scripting (XSS) attack Conduct an HTML injection attack For more information about these vulnerabilities, see the Details	https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-ciscosb-multivulns-Wwyb7s5E	O-CIS-SG22-020721/357

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			section of this advisory. **CVE ID : CVE-2021-1542**		
Improper Authenticati on	16-Jun-21	4.3	Multiple vulnerabilities in the web-based management interface of Cisco Small Business 220 Series Smart Switches could allow an attacker to do the following: Hijack a user session Execute arbitrary commands as a root user on the underlying operating system Conduct a cross-site scripting (XSS) attack Conduct an HTML injection attack For more information about these vulnerabilities, see the Details section of this advisory. **CVE ID : CVE-2021-1543**	https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-ciscosb-multivulns-Wwyb7s5E	O-CIS-SG22-020721/358
Improper Neutralizatio n of Input During Web Page Generation ('Cross-site Scripting')	16-Jun-21	4.3	Multiple vulnerabilities in the web-based management interface of Cisco Small Business 220 Series Smart Switches could allow an attacker to do the following: Hijack a user session Execute arbitrary commands as a root user on the underlying operating system Conduct a cross-site scripting (XSS) attack Conduct an HTML injection attack For more information about these vulnerabilities, see the Details section of this advisory. **CVE ID : CVE-2021-1571**	https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-ciscosb-multivulns-Wwyb7s5E	O-CIS-SG22-020721/359
sg220-26_firmware					
Improper Authenticati	16-Jun-21	9	Multiple vulnerabilities in the web-based management	https://tools.cisco.com/se	O-CIS-SG22-020721/360

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
on			interface of Cisco Small Business 220 Series Smart Switches could allow an attacker to do the following: Hijack a user session Execute arbitrary commands as a root user on the underlying operating system Conduct a cross-site scripting (XSS) attack Conduct an HTML injection attack For more information about these vulnerabilities, see the Details section of this advisory. **CVE ID : CVE-2021-1541**	curity/center /content/Cis coSecurityAd visory/cisco-sa-ciscosb-multivulns-Wwyb7s5E	
Insufficient Session Expiration	16-Jun-21	9.3	Multiple vulnerabilities in the web-based management interface of Cisco Small Business 220 Series Smart Switches could allow an attacker to do the following: Hijack a user session Execute arbitrary commands as a root user on the underlying operating system Conduct a cross-site scripting (XSS) attack Conduct an HTML injection attack For more information about these vulnerabilities, see the Details section of this advisory. **CVE ID : CVE-2021-1542**	https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-ciscosb-multivulns-Wwyb7s5E	O-CIS-SG22-020721/361
Improper Authenticati on	16-Jun-21	4.3	Multiple vulnerabilities in the web-based management interface of Cisco Small Business 220 Series Smart Switches could allow an attacker to do the following: Hijack a user session Execute arbitrary commands as a root	https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-ciscosb-multivulns-	O-CIS-SG22-020721/362

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			user on the underlying operating system Conduct a cross-site scripting (XSS) attack Conduct an HTML injection attack For more information about these vulnerabilities, see the Details section of this advisory. **CVE ID : CVE-2021-1543**	Wwyb7s5E	
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	16-Jun-21	4.3	Multiple vulnerabilities in the web-based management interface of Cisco Small Business 220 Series Smart Switches could allow an attacker to do the following: Hijack a user session Execute arbitrary commands as a root user on the underlying operating system Conduct a cross-site scripting (XSS) attack Conduct an HTML injection attack For more information about these vulnerabilities, see the Details section of this advisory. **CVE ID : CVE-2021-1571**	https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-ciscosb-multivulns-Wwyb7s5E	O-CIS-SG22-020721/363
sg220-28mp_firmware					
Improper Authentication	16-Jun-21	9	Multiple vulnerabilities in the web-based management interface of Cisco Small Business 220 Series Smart Switches could allow an attacker to do the following: Hijack a user session Execute arbitrary commands as a root user on the underlying operating system Conduct a cross-site scripting (XSS) attack Conduct an HTML	https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-ciscosb-multivulns-Wwyb7s5E	O-CIS-SG22-020721/364

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			injection attack For more information about these vulnerabilities, see the Details section of this advisory. **CVE ID : CVE-2021-1541**		
Insufficient Session Expiration	16-Jun-21	9.3	Multiple vulnerabilities in the web-based management interface of Cisco Small Business 220 Series Smart Switches could allow an attacker to do the following: Hijack a user session Execute arbitrary commands as a root user on the underlying operating system Conduct a cross-site scripting (XSS) attack Conduct an HTML injection attack For more information about these vulnerabilities, see the Details section of this advisory. **CVE ID : CVE-2021-1542**	https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-ciscosb-multivulns-Wwyb7s5E	O-CIS-SG22-020721/365
Improper Authentication	16-Jun-21	4.3	Multiple vulnerabilities in the web-based management interface of Cisco Small Business 220 Series Smart Switches could allow an attacker to do the following: Hijack a user session Execute arbitrary commands as a root user on the underlying operating system Conduct a cross-site scripting (XSS) attack Conduct an HTML injection attack For more information about these vulnerabilities, see the Details section of this advisory. **CVE ID : CVE-2021-1543**	https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-ciscosb-multivulns-Wwyb7s5E	O-CIS-SG22-020721/366

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	16-Jun-21	4.3	Multiple vulnerabilities in the web-based management interface of Cisco Small Business 220 Series Smart Switches could allow an attacker to do the following: Hijack a user session Execute arbitrary commands as a root user on the underlying operating system Conduct a cross-site scripting (XSS) attack Conduct an HTML injection attack For more information about these vulnerabilities, see the Details section of this advisory. **CVE ID : CVE-2021-1571**	https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-ciscosb-multivulns-Wwyb7s5E	O-CIS-SG22-020721/367
sg220-50p_firmware					
Improper Authentication	16-Jun-21	9	Multiple vulnerabilities in the web-based management interface of Cisco Small Business 220 Series Smart Switches could allow an attacker to do the following: Hijack a user session Execute arbitrary commands as a root user on the underlying operating system Conduct a cross-site scripting (XSS) attack Conduct an HTML injection attack For more information about these vulnerabilities, see the Details section of this advisory. **CVE ID : CVE-2021-1541**	https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-ciscosb-multivulns-Wwyb7s5E	O-CIS-SG22-020721/368
Insufficient Session Expiration	16-Jun-21	9.3	Multiple vulnerabilities in the web-based management interface of Cisco Small Business 220 Series Smart	https://tools.cisco.com/security/center/content/Cis	O-CIS-SG22-020721/369

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Switches could allow an attacker to do the following: Hijack a user session Execute arbitrary commands as a root user on the underlying operating system Conduct a cross-site scripting (XSS) attack Conduct an HTML injection attack For more information about these vulnerabilities, see the Details section of this advisory. **CVE ID : CVE-2021-1542**	coSecurityAdvisory/cisco-sa-ciscosb-multivulns-Wwyb7s5E	
Improper Authentication	16-Jun-21	4.3	Multiple vulnerabilities in the web-based management interface of Cisco Small Business 220 Series Smart Switches could allow an attacker to do the following: Hijack a user session Execute arbitrary commands as a root user on the underlying operating system Conduct a cross-site scripting (XSS) attack Conduct an HTML injection attack For more information about these vulnerabilities, see the Details section of this advisory. **CVE ID : CVE-2021-1543**	https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-ciscosb-multivulns-Wwyb7s5E	O-CIS-SG22-020721/370
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	16-Jun-21	4.3	Multiple vulnerabilities in the web-based management interface of Cisco Small Business 220 Series Smart Switches could allow an attacker to do the following: Hijack a user session Execute arbitrary commands as a root user on the underlying operating system Conduct a	https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-ciscosb-multivulns-Wwyb7s5E	O-CIS-SG22-020721/371

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			cross-site scripting (XSS) attack Conduct an HTML injection attack For more information about these vulnerabilities, see the Details section of this advisory. **CVE ID : CVE-2021-1571**		
sg220-50_firmware					
Improper Authentication	16-Jun-21	9	Multiple vulnerabilities in the web-based management interface of Cisco Small Business 220 Series Smart Switches could allow an attacker to do the following: Hijack a user session Execute arbitrary commands as a root user on the underlying operating system Conduct a cross-site scripting (XSS) attack Conduct an HTML injection attack For more information about these vulnerabilities, see the Details section of this advisory. **CVE ID : CVE-2021-1541**	https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-ciscosb-multivulns-Wwyb7s5E	O-CIS-SG22-020721/372
Insufficient Session Expiration	16-Jun-21	9.3	Multiple vulnerabilities in the web-based management interface of Cisco Small Business 220 Series Smart Switches could allow an attacker to do the following: Hijack a user session Execute arbitrary commands as a root user on the underlying operating system Conduct a cross-site scripting (XSS) attack Conduct an HTML injection attack For more information about these	https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-ciscosb-multivulns-Wwyb7s5E	O-CIS-SG22-020721/373

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			vulnerabilities, see the Details section of this advisory. **CVE ID : CVE-2021-1542**		
Improper Authentication	16-Jun-21	4.3	Multiple vulnerabilities in the web-based management interface of Cisco Small Business 220 Series Smart Switches could allow an attacker to do the following: Hijack a user session Execute arbitrary commands as a root user on the underlying operating system Conduct a cross-site scripting (XSS) attack Conduct an HTML injection attack For more information about these vulnerabilities, see the Details section of this advisory. **CVE ID : CVE-2021-1543**	https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-ciscosb-multivulns-Wwyb7s5E	O-CIS-SG22-020721/374
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	16-Jun-21	4.3	Multiple vulnerabilities in the web-based management interface of Cisco Small Business 220 Series Smart Switches could allow an attacker to do the following: Hijack a user session Execute arbitrary commands as a root user on the underlying operating system Conduct a cross-site scripting (XSS) attack Conduct an HTML injection attack For more information about these vulnerabilities, see the Details section of this advisory. **CVE ID : CVE-2021-1571**	https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-ciscosb-multivulns-Wwyb7s5E	O-CIS-SG22-020721/375
unified_contact_center_enterprise					
Improper	16-Jun-21	4.3	A vulnerability in the web-	https://tools.	O-CIS-UNIF-

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Neutralization of Input During Web Page Generation ('Cross-site Scripting')			based management interface of Cisco Unified Intelligence Center could allow an unauthenticated, remote attacker to conduct a cross-site scripting (XSS) attack against a user of the interface. This vulnerability exists because the web-based management interface does not properly validate user-supplied input. An attacker could exploit this vulnerability by persuading a user of the interface to click a crafted link. A successful exploit could allow the attacker to execute arbitrary script code in the context of the interface or access sensitive, browser-based information. **CVE ID : CVE-2021-1395**	cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-cuic-xss-csHUdtrL	020721/376
unified_contact_center_express					
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	16-Jun-21	4.3	A vulnerability in the web-based management interface of Cisco Unified Intelligence Center could allow an unauthenticated, remote attacker to conduct a cross-site scripting (XSS) attack against a user of the interface. This vulnerability exists because the web-based management interface does not properly validate user-supplied input. An attacker could exploit this vulnerability by persuading a user of the interface to click a	https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-cuic-xss-csHUdtrL	O-CIS-UNIF-020721/377

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			crafted link. A successful exploit could allow the attacker to execute arbitrary script code in the context of the interface or access sensitive, browser-based information. **CVE ID : CVE-2021-1395**		
unified_intelligence_center					
Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	16-Jun-21	4.3	A vulnerability in the web-based management interface of Cisco Unified Intelligence Center could allow an unauthenticated, remote attacker to conduct a cross-site scripting (XSS) attack against a user of the interface. This vulnerability exists because the web-based management interface does not properly validate user-supplied input. An attacker could exploit this vulnerability by persuading a user of the interface to click a crafted link. A successful exploit could allow the attacker to execute arbitrary script code in the context of the interface or access sensitive, browser-based information. **CVE ID : CVE-2021-1395**	https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-cuic-xss-csHUdtrL	O-CIS-UNIF-020721/378
contiki-ng					
contiki-ng					
Out-of-bounds Write	18-Jun-21	5	Contiki-NG is an open-source, cross-platform operating system for internet of things devices. The RPL-Classic and	https://github.com/contiki-ng/contiki-ng/pull/143	O-CON-CONT-020721/379

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			RPL-Lite implementations in the Contiki-NG operating system versions prior to 4.6 do not validate the address pointer in the RPL source routing header This makes it possible for an attacker to cause out-of-bounds writes with packets injected into the network stack. Specifically, the problem lies in the rpl_ext_header_srh_update function in the two rpl-ext-header.c modules for RPL-Classic and RPL-Lite respectively. The addr_ptr variable is calculated using an unvalidated CMPR field value from the source routing header. An out-of-bounds write can be triggered on line 151 in os/net/routing/rpl-lite/rpl-ext-header.c and line 261 in os/net/routing/rpl-classic/rpl-ext-header.c, which contain the following memcpy call with addr_ptr as destination. The problem has been patched in Contiki-NG 4.6. Users can apply a patch out-of-band as a workaround. **CVE ID : CVE-2021-21257**	1, https://github.com/contiki-ng/contiki-ng/security/advisories/GHSA-mvc7-9p4q-c5cm	
Loop with Unreachable Exit Condition ('Infinite Loop')	18-Jun-21	7.8	Contiki-NG is an open-source, cross-platform operating system for internet of things devices. In verions prior to 4.6, an attacker can perform a denial-of-service attack by triggering an infinite loop in the processing of IPv6	https://github.com/contiki-ng/contiki-ng/security/advisories/GHSA-rr5j-j8m8-fc4f	O-CON-CONT-020721/380

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			neighbor solicitation (NS) messages. This type of attack can effectively shut down the operation of the system because of the cooperative scheduling used for the main parts of Contiki-NG and its communication stack. The problem has been patched in Contiki-NG 4.6. Users can apply the patch for this vulnerability out-of-band as a workaround. **CVE ID : CVE-2021-21279**		
Out-of-bounds Write	18-Jun-21	7.5	Contiki-NG is an open-source, cross-platform operating system for internet of things devices. It is possible to cause an out-of-bounds write in versions of Contiki-NG prior to 4.6 when transmitting a 6LoWPAN packet with a chain of extension headers. Unfortunately, the written header is not checked to be within the available space, thereby making it possible to write outside the buffer. The problem has been patched in Contiki-NG 4.6. Users can apply the patch for this vulnerability out-of-band as a workaround. **CVE ID : CVE-2021-21280**	https://github.com/contiki-ng/contiki-ng/pull/1409, https://github.com/contiki-ng/contiki-ng/security/advisories/GHSA-r768-hrhf-v592	O-CON-CONT-020721/381
Buffer Copy without Checking Size of Input ('Classic Buffer	18-Jun-21	7.5	Contiki-NG is an open-source, cross-platform operating system for internet of things devices. A buffer overflow vulnerability exists in Contiki-NG versions prior to	https://github.com/contiki-ng/contiki-ng/pull/1366, https://githu	O-CON-CONT-020721/382

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Overflow')			4.6. After establishing a TCP socket using the tcp-socket library, it is possible for the remote end to send a packet with a data offset that is unvalidated. The problem has been patched in Contiki-NG 4.6. Users can apply the patch for this vulnerability out-of-band as a workaround. **CVE ID : CVE-2021-21281**	b.com/contiki-ng/contiki-ng/security/advisories/GHSA-mc42-fqfr-h9fp	
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	18-Jun-21	7.5	Contiki-NG is an open-source, cross-platform operating system for internet of things devices. In versions prior to 4.5, buffer overflow can be triggered by an input packet when using either of Contiki-NG's two RPL implementations in source-routing mode. The problem has been patched in Contiki-NG 4.5. Users can apply the patch for this vulnerability out-of-band as a workaround. **CVE ID : CVE-2021-21282**	https://github.com/contiki-ng/contiki-ng/pull/1183, https://github.com/contiki-ng/contiki-ng/security/advisories/GHSA-6xf2-77gf-fgjx	O-CON-CONT-020721/383
Out-of-bounds Read	18-Jun-21	6.4	Contiki-NG is an open-source, cross-platform operating system for Next-Generation IoT devices. An out-of-bounds read can be triggered by 6LoWPAN packets sent to devices running Contiki-NG 4.6 and prior. The IPv6 header decompression function (<code>uncompress_hdr_iphc</code>) does not perform proper boundary checks when reading from the	https://github.com/contiki-ng/contiki-ng/security/advisories/GHSA-hhwj-2p59-v8p9, https://github.com/contiki-ng/contiki-ng/pull/1482	O-CON-CONT-020721/384

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			packet buffer. Hence, it is possible to construct a compressed 6LoWPAN packet that will read more bytes than what is available from the packet buffer. As of time of publication, there is not a release with a patch available. Users can apply the patch for this vulnerability out-of-band as a workaround. **CVE ID : CVE-2021-21410**		
Dlink					
dir-2640-us_firmware					
Out-of-bounds Write	16-Jun-21	3.6	D-Link DIR-2640-US 1.01B04 is vulnerable to Buffer Overflow. There are multiple out-of-bounds vulnerabilities in some processes of D-Link AC2600(DIR-2640). Local ordinary users can overwrite the global variables in the .bss section, causing the process crashes or changes. **CVE ID : CVE-2021-34201**	https://www.dlink.com/en/security-bulletin/	O-DLI-DIR--020721/385
Out-of-bounds Write	16-Jun-21	7.2	There are multiple out-of-bounds vulnerabilities in some processes of D-Link AC2600(DIR-2640) 1.01B04. Ordinary permissions can be elevated to administrator permissions, resulting in local arbitrary code execution. An attacker can combine other vulnerabilities to further achieve the purpose of remote code execution. **CVE ID : CVE-2021-34202**	https://www.dlink.com/en/security-bulletin/, http://d-link.com	O-DLI-DIR--020721/386

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Incorrect Authorization	16-Jun-21	4.8	D-Link DIR-2640-US 1.01B04 is vulnerable to Incorrect Access Control. Router ac2600 (dir-2640-us), when setting PPPoE, will start quagga process in the way of whole network monitoring, and this function uses the original default password and port. An attacker can easily use telnet to log in, modify routing information, monitor the traffic of all devices under the router, hijack DNS and phishing attacks. In addition, this interface is likely to be questioned by customers as a backdoor, because the interface should not be exposed. **CVE ID : CVE-2021-34203**	https://www.dlink.com/en/security-bulletin/, http://d-link.com	O-DLI-DIR--020721/387
Insufficiently Protected Credentials	16-Jun-21	7.2	D-Link DIR-2640-US 1.01B04 is affected by Insufficiently Protected Credentials. D-Link AC2600(DIR-2640) stores the device system account password in plain text. It does not use linux user management. In addition, the passwords of all devices are the same, and they cannot be modified by normal users. An attacker can easily log in to the target router through the serial port and obtain root privileges. **CVE ID : CVE-2021-34204**	https://www.dlink.com/en/security-bulletin/	O-DLI-DIR--020721/388
GE					
reason_rpv311_firmware					

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Use of Hard-coded Credentials	16-Jun-21	7.5	This vulnerability allows remote attackers to execute arbitrary code on affected installations of GE Reason RPV311 14A03. Authentication is not required to exploit this vulnerability. The specific flaw exists within the firmware and filesystem of the device. The firmware and filesystem contain hard-coded default credentials. An attacker can leverage this vulnerability to execute code in the context of the download user. Was ZDI-CAN-11852. **CVE ID : CVE-2021-31477**	https://www.gegridsolutions.com/products/support/GES-2021-005%20-%20RPV311%20Security%20Notice.pdf	O-GE-REAS-020721/389
Google					
android					
Improper Handling of Exceptional Conditions	21-Jun-21	7.2	In updateDrawable of StatusBarIconView.java, there is a possible permission bypass due to an uncaught exception. This could lead to local escalation of privilege by running foreground services without notifying the user, with User execution privileges needed. User interaction is not needed for exploitation.Product: AndroidVersions: Android-10 Android-11 Android-8.1 Android-9Android ID: A-169255797 **CVE ID : CVE-2021-0478**	https://source.android.com/security/bulletin/2021-06-01	O-GOO-ANDR-020721/390
Out-of-	21-Jun-21	3.3	In avrc_pars_browse_rsp of	https://sour	O-GOO-

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
bounds Read			avrc_pars_ct.cc, there is a possible out of bounds read due to a missing bounds check. This could lead to remote information disclosure over Bluetooth with no additional execution privileges needed. User interaction is not needed for exploitation.Product: AndroidVersions: Android-11Android ID: A-179162665 **CVE ID : CVE-2021-0504**	ce.android.com/security/bulletin/2021-06-01	ANDR-020721/391
Incorrect Authorization	21-Jun-21	7.2	In the Settings app, there is a possible way to disable an always-on VPN due to a missing permission check. This could lead to local escalation of privilege with no additional execution privileges needed. User interaction is not needed for exploitation.Product: AndroidVersions: Android-11Android ID: A-179975048 **CVE ID : CVE-2021-0505**	https://source.android.com/security/bulletin/2021-06-01	O-GOO-ANDR-020721/392
Improper Restriction of Rendered UI Layers or Frames	21-Jun-21	6.9	In ActivityPicker.java, there is a possible bypass of user interaction in intent resolution due to a tapjacking/overlay attack. This could lead to local escalation of privilege with User execution privileges needed. User interaction is needed for exploitation.Product: AndroidVersions: Android-10 Android-11 Android-8.1 Android-9Android ID: A-	https://source.android.com/security/bulletin/2021-06-01	O-GOO-ANDR-020721/393

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			181962311 **CVE ID : CVE-2021-0506**		
Out-of-bounds Write	21-Jun-21	8.3	In handle_rc_metamsg_cmd of btif_rc.cc, there is a possible out of bounds write due to a missing bounds check. This could lead to remote code execution over Bluetooth with no additional execution privileges needed. User interaction is not needed for exploitation.Product: AndroidVersions: Android-11 Android-8.1 Android-9 Android-10Android ID: A-181860042 **CVE ID : CVE-2021-0507**	https://source.android.com/security/bulletin/2021-06-01	O-GOO-ANDR-020721/394
Concurrent Execution using Shared Resource with Improper Synchronization ('Race Condition')	21-Jun-21	6.9	In various functions of DrmPlugin.cpp, there is a possible use after free due to a race condition. This could lead to local escalation of privilege with no additional execution privileges needed. User interaction is not needed for exploitation.Product: AndroidVersions: Android-8.1 Android-9 Android-10 Android-11Android ID: A-176444154 **CVE ID : CVE-2021-0508**	https://source.android.com/security/bulletin/2021-06-01	O-GOO-ANDR-020721/395
Concurrent Execution using Shared Resource with Improper Synchronizat	21-Jun-21	4.4	In various functions of CryptoPlugin.cpp, there is a possible use after free due to a race condition. This could lead to local escalation of privilege with no additional execution privileges needed.	https://source.android.com/security/bulletin/2021-06-01	O-GOO-ANDR-020721/396

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
ion ('Race Condition')			User interaction is not needed for exploitation.Product: AndroidVersions: Android-9 Android-10 Android-11 Android-8.1Android ID: A-176444161 **CVE ID : CVE-2021-0509**		
Out-of-bounds Write	21-Jun-21	4.6	In decrypt_1_2 of CryptoPlugin.cpp, there is a possible out of bounds write due to an integer overflow. This could lead to local escalation of privilege with no additional execution privileges needed. User interaction is not needed for exploitation.Product: AndroidVersions: Android-9 Android-10 Android-11 Android-8.1Android ID: A-176444622 **CVE ID : CVE-2021-0510**	https://source.android.com/security/bulletin/2021-06-01	O-GOO-ANDR-020721/397
Improper Input Validation	21-Jun-21	4.6	In Dex2oat of dex2oat.cc, there is a possible way to inject bytecode into an app due to improper input validation. This could lead to local escalation of privilege with no additional execution privileges needed. User interaction is not needed for exploitation.Product: AndroidVersions: Android-9 Android-10 Android-11Android ID: A-178055795 **CVE ID : CVE-2021-0511**	https://source.android.com/security/bulletin/2021-06-01	O-GOO-ANDR-020721/398
Out-of-bounds	21-Jun-21	4.6	In __hidinput_change_resolution	https://source.android.co	O-GOO-ANDR-

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Write			_multipliers of hid-input.c, there is a possible out of bounds write due to a heap buffer overflow. This could lead to local escalation of privilege with no additional execution privileges needed. User interaction is not needed for exploitation.Product: AndroidVersions: Android kernelAndroid ID: A-173843328References: Upstream kernel **CVE ID : CVE-2021-0512**	m/security/bulletin/2021-06-01	020721/399
Improper Privilege Management	21-Jun-21	4.6	In deleteNotificationChannel and related functions of NotificationManagerService.java, there is a possible permission bypass due to improper state validation. This could lead to local escalation of privilege via hidden services with no additional execution privileges needed. User interaction is not needed for exploitation.Product: AndroidVersions: Android-9 Android-10 Android-11 Android-8.1Android ID: A-156090809 **CVE ID : CVE-2021-0513**	https://source.android.com/security/bulletin/2021-06-01	O-GOO-ANDR-020721/400
Out-of-bounds Read	21-Jun-21	7.5	In p2p_process_prov_disc_req of p2p_pd.c, there is a possible out of bounds read and write due to a use after free. This could lead to remote escalation of privilege with no additional execution	https://source.android.com/security/bulletin/2021-06-01	O-GOO-ANDR-020721/401

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			privileges needed. User interaction is not needed for exploitation.Product: AndroidVersions: Android-11 Android-8.1 Android-9 Android-10Android ID: A-181660448 **CVE ID : CVE-2021-0516**		
Always-Incorrect Control Flow Implementation	21-Jun-21	5	In updateCapabilities of ConnectivityService.java, there is a possible incorrect network state determination due to a logic error in the code. This could lead to biasing of networking tasks to occur on non-VPN networks, which could lead to remote information disclosure, with no additional execution privileges needed. User interaction is not needed for exploitation.Product: AndroidVersions: Android-11Android ID: A-179053823 **CVE ID : CVE-2021-0517**	https://source.android.com/security/bulletin/2021-06-01	O-GOO-ANDR-020721/402
Concurrent Execution using Shared Resource with Improper Synchronization ('Race Condition')	21-Jun-21	4.4	In several functions of MemoryFileSystem.cpp and related files, there is a possible use after free due to a race condition. This could lead to local escalation of privilege with no additional execution privileges needed. User interaction is not needed for exploitation.Product: AndroidVersions: Android-11 Android-10Android ID: A-176237595	https://source.android.com/security/bulletin/2021-06-01	O-GOO-ANDR-020721/403

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2021-0520		
Missing Authorization	21-Jun-21	2.1	In getAllPackages of PackageManagerService, there is a possible information disclosure due to a missing permission check. This could lead to local information disclosure of cross-user permissions with no additional execution privileges needed. User interaction is not needed for exploitation.Product: AndroidVersions: Android-11 Android-8.1 Android-9 Android-10Android ID: A-174661955 **CVE ID : CVE-2021-0521**	https://source.android.com/security/bulletin/2021-06-01	O-GOO-ANDR-020721/404
Out-of-bounds Read	21-Jun-21	5	In ConnectionHandler::SdpCb of connection_handler.cc, there is a possible out of bounds read due to a use after free. This could lead to remote information disclosure with no additional execution privileges needed. User interaction is not needed for exploitation.Product: AndroidVersions: Android-11 Android-9 Android-10Android ID: A-174182139 **CVE ID : CVE-2021-0522**	https://source.android.com/security/bulletin/2021-06-01	O-GOO-ANDR-020721/405
Improper Restriction of Rendered UI Layers or Frames	21-Jun-21	4.4	In onCreate of WifiScanModeActivity.java, there is a possible way to enable Wi-Fi scanning without user consent due to a tapjacking/overlay attack.	https://source.android.com/security/bulletin/2021-06-01	O-GOO-ANDR-020721/406

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			This could lead to local escalation of privilege with User execution privileges needed. User interaction is needed for exploitation.Product: AndroidVersions: Android-10 Android-11Android ID: A-174047492 **CVE ID : CVE-2021-0523**		
Out-of-bounds Write	21-Jun-21	4.6	In memory management driver, there is a possible out of bounds write due to a use after free. This could lead to local escalation of privilege with no additional execution privileges needed. User interaction is not needed for exploitation.Product: AndroidVersions: Android SoCAndroid ID: A-185193929 **CVE ID : CVE-2021-0525**	https://source.android.com/security/bulletin/2021-06-01	O-GOO-ANDR-020721/407
Out-of-bounds Write	21-Jun-21	4.6	In memory management driver, there is a possible out of bounds write due to uninitialized data. This could lead to local escalation of privilege with no additional execution privileges needed. User interaction is not needed for exploitation.Product: AndroidVersions: Android SoCAndroid ID: A-185195264 **CVE ID : CVE-2021-0526**	https://source.android.com/security/bulletin/2021-06-01	O-GOO-ANDR-020721/408
Use After Free	21-Jun-21	4.6	In memory management driver, there is a possible memory corruption due to a use after free. This could lead	https://source.android.com/security/bulletin/202	O-GOO-ANDR-020721/409

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			to local escalation of privilege with no additional execution privileges needed. User interaction is not needed for exploitation.Product: AndroidVersions: Android SoCAndroid ID: A-185193931 **CVE ID : CVE-2021-0527**	1-06-01	
Double Free	21-Jun-21	4.6	In memory management driver, there is a possible memory corruption due to a double free. This could lead to local escalation of privilege with no additional execution privileges needed. User interaction is not needed for exploitation.Product: AndroidVersions: Android SoCAndroid ID: A-185195266 **CVE ID : CVE-2021-0528**	https://source.android.com/security/bulletin/2021-06-01	O-GOO-ANDR-020721/410
Improper Locking	21-Jun-21	4.6	In memory management driver, there is a possible memory corruption due to improper locking. This could lead to local escalation of privilege with no additional execution privileges needed. User interaction is not needed for exploitation.Product: AndroidVersions: Android SoCAndroid ID: A-185195268 **CVE ID : CVE-2021-0529**	https://source.android.com/security/bulletin/2021-06-01	O-GOO-ANDR-020721/411
Out-of-bounds Write	21-Jun-21	4.6	In memory management driver, there is a possible out of bounds write due to uninitialized data. This could lead to local escalation of privilege with no additional	https://source.android.com/security/bulletin/2021-06-01	O-GOO-ANDR-020721/412

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			execution privileges needed. User interaction is not needed for exploitation.Product: AndroidVersions: Android SoCAndroid ID: A-185196175 **CVE ID : CVE-2021-0530**		
Use After Free	21-Jun-21	4.6	In memory management driver, there is a possible memory corruption due to a use after free. This could lead to local escalation of privilege with no additional execution privileges needed. User interaction is not needed for exploitation.Product: AndroidVersions: Android SoCAndroid ID: A-185195272 **CVE ID : CVE-2021-0531**	https://source.android.com/security/bulletin/2021-06-01	O-GOO-ANDR-020721/413
Concurrent Execution using Shared Resource with Improper Synchronization ('Race Condition')	21-Jun-21	4.4	In memory management driver, there is a possible memory corruption due to a race condition. This could lead to local escalation of privilege with no additional execution privileges needed. User interaction is not needed for exploitation.Product: AndroidVersions: Android SoCAndroid ID: A-185196177 **CVE ID : CVE-2021-0532**	https://source.android.com/security/bulletin/2021-06-01	O-GOO-ANDR-020721/414
Concurrent Execution using Shared Resource with Improper Synchronizat	21-Jun-21	4.4	In memory management driver, there is a possible memory corruption due to a race condition. This could lead to local escalation of privilege with no additional execution privileges needed.	https://source.android.com/security/bulletin/2021-06-01	O-GOO-ANDR-020721/415

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
ion ('Race Condition')			User interaction is not needed for exploitation.Product: AndroidVersions: Android SoCAndroid ID: A-185193932 **CVE ID : CVE-2021-0533**		
Insecure Default Initialization of Resource	22-Jun-21	4.6	In permission declarations of DeviceAdminReceiver.java, there is a possible lack of broadcast protection due to an insecure default value. This could lead to local escalation of privilege with no additional execution privileges needed. User interaction is not needed for exploitation.Product: AndroidVersions: Android-11Android ID: A-170639543 **CVE ID : CVE-2021-0534**	https://source.android.com/security/bulletin/pixel/2021-06-01	O-GOO-ANDR-020721/416
Use After Free	22-Jun-21	4.6	In wpas_ctrl_msg_queue_timeout of ctrl_iface_unix.c, there is a possible memory corruption due to a use after free. This could lead to local escalation of privilege with System execution privileges needed. User interaction is not needed for exploitation.Product: AndroidVersions: Android-11Android ID: A-168314741 **CVE ID : CVE-2021-0535**	https://source.android.com/security/bulletin/pixel/2021-06-01	O-GOO-ANDR-020721/417
Externally Controlled Reference to a Resource in Another	22-Jun-21	4.6	In dropFile of WiFiInstaller, there is a way to delete files accessible to CertInstaller due to a confused deputy. This could lead to local	https://source.android.com/security/bulletin/pixel/2021-06-	O-GOO-ANDR-020721/418

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Sphere			escalation of privilege with no additional execution privileges needed. User interaction is not needed for exploitation.Product: AndroidVersions: Android-11Android ID: A-176756691 **CVE ID : CVE-2021-0536**	01	
Improper Restriction of Rendered UI Layers or Frames	22-Jun-21	4.4	In onCreate of WiFiInstaller.java, there is a possible way to install a malicious Hotspot 2.0 configuration due to a tapjacking/overlay attack. This could lead to local escalation of privilege with User execution privileges needed. User interaction is needed for exploitation.Product: AndroidVersions: Android-11Android ID: A-176756141 **CVE ID : CVE-2021-0537**	https://source.android.com/security/bulletin/pixel/2021-06-01	O-GOO-ANDR-020721/419
Improper Restriction of Rendered UI Layers or Frames	22-Jun-21	4.4	In onCreate of EmergencyCallbackModeExitDialog.java, there is a possible exit of emergency callback mode due to a tapjacking/overlay attack. This could lead to local escalation of privilege with User execution privileges needed. User interaction is needed for exploitation.Product: AndroidVersions: Android-11Android ID: A-178821491 **CVE ID : CVE-2021-0538**	https://source.android.com/security/bulletin/pixel/2021-06-01	O-GOO-ANDR-020721/420
Incorrect	22-Jun-21	4.6	In archiveStoredConversation	https://sour	O-GOO-

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Permission Assignment for Critical Resource			of MmsService.java, there is a possible way to archive message conversation without user consent due to a missing permission check. This could lead to local escalation of privilege with no additional execution privileges needed. User interaction is not needed for exploitation.Product: AndroidVersions: Android-11Android ID: A-180419673 **CVE ID : CVE-2021-0539**	ce.android.com/security/bulletin/pixel/2021-06-01	ANDR-020721/421
Out-of-bounds Write	22-Jun-21	4.6	In halWrapperDataCallback of hal_wrapper.cc, there is a possible out of bounds write due to a missing bounds check. This could lead to local escalation of privilege with System execution privileges needed. User interaction is not needed for exploitation.Product: AndroidVersions: Android-11Android ID: A-169328517 **CVE ID : CVE-2021-0540**	https://source.android.com/security/bulletin/pixel/2021-06-01	O-GOO-ANDR-020721/422
Out-of-bounds Read	22-Jun-21	2.1	In phNxpNciHal_ext_process_nfc_init_rsp of phNxpNciHal_ext.cc, there is a possible out of bounds read due to a missing bounds check. This could lead to local information disclosure in the NFC server with System execution privileges needed. User interaction is not needed for exploitation.Product:	https://source.android.com/security/bulletin/pixel/2021-06-01	O-GOO-ANDR-020721/423

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			AndroidVersions: Android-11Android ID: A-169258455 **CVE ID : CVE-2021-0541**		
Improper Preservation of Permissions	22-Jun-21	2.1	In updateNotification of BeamTransferManager.java, there is a missing permission check. This could lead to local information disclosure of paired Bluetooth addresses with no additional execution privileges needed. User interaction is needed for exploitation.Product: AndroidVersions: Android-11Android ID: A-168712890 **CVE ID : CVE-2021-0542**	https://source.android.com/security/bulletin/pixel/2021-06-01	O-GOO-ANDR-020721/424
Out-of-bounds Write	22-Jun-21	4.6	In phNxpNciHal_process_ext_rsp of phNxpNciHal_ext.cc, there is a possible out of bounds write due to an integer overflow. This could lead to local escalation of privilege with System execution privileges needed. User interaction is not needed for exploitation.Product: AndroidVersions: Android-11Android ID: A-169258743 **CVE ID : CVE-2021-0543**	https://source.android.com/security/bulletin/pixel/2021-06-01	O-GOO-ANDR-020721/425
Out-of-bounds Write	22-Jun-21	4.6	In phNxpNciHal_print_res_status of phNxpNciHal.cc, there is a possible out of bounds write due to a missing bounds check. This could lead to local escalation of privilege with System execution privileges needed. User	https://source.android.com/security/bulletin/pixel/2021-06-01	O-GOO-ANDR-020721/426

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			interaction is not needed for exploitation.Product: AndroidVersions: Android-11Android ID: A-169257710 **CVE ID : CVE-2021-0544**		
Out-of-bounds Write	22-Jun-21	4.6	In phNxpNciHal_print_res_status of phNxpNciHal.cc, there is a possible out of bounds write due to a missing bounds check. This could lead to local escalation of privilege in the NFC server with System execution privileges needed. User interaction is not needed for exploitation.Product: AndroidVersions: Android-11Android ID: A-169258884 **CVE ID : CVE-2021-0545**	https://source.android.com/security/bulletin/pixel/2021-06-01	O-GOO-ANDR-020721/427
Out-of-bounds Write	22-Jun-21	4.6	In phNxpNciHal_print_res_status of phNxpNciHal.cc, there is a possible out of bounds write due to a missing bounds check. This could lead to local escalation of privilege with System execution privileges needed. User interaction is not needed for exploitation.Product: AndroidVersions: Android-11Android ID: A-169258733 **CVE ID : CVE-2021-0546**	https://source.android.com/security/bulletin/pixel/2021-06-01	O-GOO-ANDR-020721/428
Missing Authorization	22-Jun-21	4.6	In onReceive of NetInitiatedActivity.java, there is a possible way to supply an attacker-controlled value to a GPS HAL handler	https://source.android.com/security/bulletin/pixel/2021-06-	O-GOO-ANDR-020721/429

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			due to a missing permission check. This could lead to local escalation of privilege that may result in undefined behavior in some HAL implementations with no additional execution privileges needed. User interaction is not needed for exploitation.Product: AndroidVersions: Android-11Android ID: A-174151048 **CVE ID : CVE-2021-0547**	01	
Out-of-bounds Write	22-Jun-21	4.6	In rw_i93_send_to_lower of rw_i93.cc, there is a possible out of bounds write due to a missing bounds check. This could lead to local escalation of privilege with no additional execution privileges needed. User interaction is not needed for exploitation.Product: AndroidVersions: Android-11Android ID: A-157650357 **CVE ID : CVE-2021-0548**	https://source.android.com/security/bulletin/pixel/2021-06-01	O-GOO-ANDR-020721/430
Insertion of Sensitive Information into Log File	22-Jun-21	2.1	In sspRequestCallback of BondStateMachine.java, there is a possible leak of Bluetooth MAC addresses due to log information disclosure. This could lead to local information disclosure with System execution privileges needed. User interaction is not needed for exploitation.Product: AndroidVersions: Android-11Android ID: A-183961896	https://source.android.com/security/bulletin/pixel/2021-06-01	O-GOO-ANDR-020721/431

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2021-0549		
Externally Controlled Reference to a Resource in Another Sphere	22-Jun-21	4.6	In onLoadFailed of AnnotateActivity.java, there is a possible way to gain WRITE_EXTERNAL_STORAGE permissions without user consent due to a confused deputy. This could lead to local escalation of privilege with no additional execution privileges needed. User interaction is not needed for exploitation.Product: AndroidVersions: Android-11Android ID: A-179688673 **CVE ID : CVE-2021-0550**	https://source.android.com/security/bulletin/pixel/2021-06-01	O-GOO-ANDR-020721/432
Improper Input Validation	22-Jun-21	4.3	In bind of MediaControlPanel.java, there is a possible way to lock up the system UI using a malicious media file due to improper input validation. This could lead to remote denial of service with no additional execution privileges needed. User interaction is needed for exploitation.Product: AndroidVersions: Android-11Android ID: A-180518039 **CVE ID : CVE-2021-0551**	https://source.android.com/security/bulletin/pixel/2021-06-01	O-GOO-ANDR-020721/433
Exposure of Resource to Wrong Sphere	22-Jun-21	2.1	In getEndItemSliceAction of MediaOutputSlice.java, there is a possible permission bypass due to an unsafe PendingIntent. This could lead to local information disclosure with User execution privileges needed.	https://source.android.com/security/bulletin/pixel/2021-06-01	O-GOO-ANDR-020721/434

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			User interaction is not needed for exploitation.Product: AndroidVersions: Android-11Android ID: A-175124820 **CVE ID : CVE-2021-0552**		
Improper Privilege Management	22-Jun-21	4.4	In onBindViewHolder of AppSwitchPreference.java, there is a possible bypass of device admin setttings due to unclear UI. This could lead to local escalation of privilege with User execution privileges needed. User interaction is needed for exploitation.Product: AndroidVersions: Android-11Android ID: A-169936038 **CVE ID : CVE-2021-0553**	https://source.android.com/security/bulletin/pixel/2021-06-01	O-GOO-ANDR-020721/435
Missing Authorization	22-Jun-21	2.1	In isBackupServiceActive of BackupManagerService.java, there is a missing permission check. This could lead to local information disclosure with no additional execution privileges needed. User interaction is not needed for exploitation.Product: AndroidVersions: Android-11Android ID: A-158482162 **CVE ID : CVE-2021-0554**	https://source.android.com/security/bulletin/pixel/2021-06-01	O-GOO-ANDR-020721/436
NULL Pointer Dereference	22-Jun-21	5	In RenderStruct of protostream_objectsource.cc, there is a possible crash due to a missing null check. This could lead to remote denial of service with no additional execution privileges needed. User interaction is not	https://source.android.com/security/bulletin/pixel/2021-06-01	O-GOO-ANDR-020721/437

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			needed for exploitation.Product: AndroidVersions: Android-11Android ID: A-179161711 **CVE ID : CVE-2021-0555**		
Out-of-bounds Read	22-Jun-21	2.1	In getBlockSum of fastcodemb.cpp, there is a possible out of bounds read due to a heap buffer overflow. This could lead to local information disclosure with no additional execution privileges needed. User interaction is not needed for exploitation.Product: AndroidVersions: Android-11Android ID: A-172716941 **CVE ID : CVE-2021-0556**	https://source.android.com/security/bulletin/pixel/2021-06-01	O-GOO-ANDR-020721/438
Out-of-bounds Write	22-Jun-21	6.8	In setRange of ABuffer.cpp, there is a possible out of bounds write due to an integer overflow. This could lead to remote code execution with no additional execution privileges needed. User interaction is needed for exploitation.Product: AndroidVersions: Android-11Android ID: A-179046129 **CVE ID : CVE-2021-0557**	https://source.android.com/security/bulletin/pixel/2021-06-01	O-GOO-ANDR-020721/439
Out-of-bounds Read	22-Jun-21	4.3	In fillMainDataBuf of pvmp3_framedecoder.cpp, there is a possible out of bounds read due to a heap buffer overflow. This could lead to remote information disclosure with no additional execution privileges needed. User interaction is needed for	https://source.android.com/security/bulletin/pixel/2021-06-01	O-GOO-ANDR-020721/440

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			exploitation.Product: AndroidVersions: Android-11Android ID: A-173473906 **CVE ID : CVE-2021-0558**		
Out-of-bounds Read	22-Jun-21	4.3	In Lag_max of p_ol_wgh.cpp, there is a possible out of bounds read due to a missing bounds check. This could lead to remote information disclosure with no additional execution privileges needed. User interaction is needed for exploitation.Product: AndroidVersions: Android-11Android ID: A-172312730 **CVE ID : CVE-2021-0559**	https://source.android.com/security/bulletin/pixel/2021-06-01	O-GOO-ANDR-020721/441
Out-of-bounds Write	22-Jun-21	2.1	In append_to_verify_fifo_interleaved_ of stream_encoder.c, there is a possible out of bounds write due to a missing bounds check. This could lead to local information disclosure with no additional execution privileges needed. User interaction is not needed for exploitation.Product: AndroidVersions: Android-11Android ID: A-174302683 **CVE ID : CVE-2021-0561**	https://source.android.com/security/bulletin/pixel/2021-06-01	O-GOO-ANDR-020721/442
Out-of-bounds Read	22-Jun-21	2.1	In RasterIntraUpdate of motion_est.cpp, there is a possible out of bounds read due to an incorrect bounds check. This could lead to local information disclosure with no additional execution privileges needed. User	https://source.android.com/security/bulletin/pixel/2021-06-01	O-GOO-ANDR-020721/443

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			interaction is not needed for exploitation.Product: AndroidVersions: Android-11Android ID: A-176084648 **CVE ID : CVE-2021-0562**		
Out-of-bounds Read	22-Jun-21	2.1	In ih264e_fmt_conv_422i_to_420sp of ih264e_fmt_conv.c, there is a possible out of bounds read due to a heap buffer overflow. This could lead to local information disclosure with no additional execution privileges needed. User interaction is not needed for exploitation.Product: AndroidVersions: Android-11Android ID: A-172908358 **CVE ID : CVE-2021-0563**	https://source.android.com/security/bulletin/pixel/2021-06-01	O-GOO-ANDR-020721/444
Concurrent Execution using Shared Resource with Improper Synchronization ('Race Condition')	22-Jun-21	4.4	In decrypt of CryptoPlugin.cpp, there is a possible use-after-free due to a race condition. This could lead to local escalation of privilege with System execution privileges needed. User interaction is not needed for exploitation.Product: AndroidVersions: Android-11Android ID: A-176495665 **CVE ID : CVE-2021-0564**	https://source.android.com/security/bulletin/pixel/2021-06-01	O-GOO-ANDR-020721/445
Concurrent Execution using Shared Resource with Improper	22-Jun-21	4.4	In wrapUserThread of AudioStream.cpp, there is a possible use after free due to a race condition. This could lead to local escalation of privilege with no additional	https://source.android.com/security/bulletin/pixel/2021-06-01	O-GOO-ANDR-020721/446

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Synchronization ('Race Condition')			execution privileges needed. User interaction is not needed for exploitation.Product: AndroidVersions: Android-11Android ID: A-174801970 **CVE ID : CVE-2021-0565**		
Out-of-bounds Read	22-Jun-21	2.1	In accessAudioHalPidscpp of TimeCheck.cpp, there is a possible out of bounds read due to a missing bounds check. This could lead to local information disclosure with System execution privileges needed. User interaction is not needed for exploitation.Product: AndroidVersions: Android-11Android ID: A-175894436 **CVE ID : CVE-2021-0566**	https://source.android.com/security/bulletin/pixel/2021-06-01	O-GOO-ANDR-020721/447
Improper Neutralization of Special Elements in Output Used by a Downstream Component ('Injection')	22-Jun-21	4.6	In isRestricted of RemoteViews.java, there is a possible way to inject font files due to a permissions bypass. This could lead to local escalation of privilege with no additional execution privileges needed. User interaction is not needed for exploitation.Product: AndroidVersions: Android-11Android ID: A-179461812 **CVE ID : CVE-2021-0567**	https://source.android.com/security/bulletin/pixel/2021-06-01	O-GOO-ANDR-020721/448
Missing Authorization	22-Jun-21	4.6	In onReceive of DevicePolicyManagerService.java, there is a possible enabling of disabled profiles due to a missing permission check. This could lead to local	https://source.android.com/security/bulletin/pixel/2021-06-01	O-GOO-ANDR-020721/449

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			escalation of privilege with no additional execution privileges needed. User interaction is not needed for exploitation.Product: AndroidVersions: Android-11Android ID: A-170121238 **CVE ID : CVE-2021-0568**		
Improper Restriction of Rendered UI Layers or Frames	22-Jun-21	1.9	In onStart of ContactsDumpActivity.java, there is possible access to contacts due to a tapjacking/overlay attack. This could lead to local information disclosure with User execution privileges needed. User interaction is needed for exploitation.Product: AndroidVersions: Android-11Android ID: A-174045870 **CVE ID : CVE-2021-0569**	https://source.android.com/security/bulletin/pixel/2021-06-01	O-GOO-ANDR-020721/450
Improper Authentication	22-Jun-21	4.6	In sendBugreportNotification of BugreportProgressService.java, there is a possible permission bypass due to an unsafe PendingIntent. This could lead to local escalation of privilege with User execution privileges needed. User interaction is not needed for exploitation.Product: AndroidVersions: Android-11Android ID: A-178803845 **CVE ID : CVE-2021-0570**	https://source.android.com/security/bulletin/pixel/2021-06-01	O-GOO-ANDR-020721/451
Improper Authenticati	22-Jun-21	4.6	In ActivityTaskManagerService.	https://source.android.co	O-GOO-ANDR-

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
on			startActivity() and AppTaskImpl.startActivity() of ActivityTaskManagerService.java and AppTaskImpl.java, there is possible access to restricted activities due to a permissions bypass. This could lead to local escalation of privilege with no additional execution privileges needed. User interaction is not needed for exploitation.Product: AndroidVersions: Android-11Android ID: A-137395936 **CVE ID : CVE-2021-0571**	m/security/bulletin/pixel/2021-06-01	020721/452
Improper Authentication	22-Jun-21	2.1	In doNotification of AccountManagerService.java, there is a possible permission bypass due to an unsafe PendingIntent. This could lead to local information disclosure with User execution privileges needed. User interaction is not needed for exploitation.Product: AndroidVersions: Android-11Android ID: A-177931355 **CVE ID : CVE-2021-0572**	https://source.android.com/security/bulletin/pixel/2021-06-01	O-GOO-ANDR-020721/453
Out-of-bounds Read	22-Jun-21	4.9	In pfkey_dump of af_key.c, there is a possible out-of-bounds read due to a missing bounds check. This could lead to local information disclosure in the kernel with System execution privileges needed. User interaction is not needed for	https://source.android.com/security/bulletin/pixel/2021-06-01	O-GOO-ANDR-020721/454

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			exploitation.Product: AndroidVersions: Android kernelAndroid ID: A-110373476 **CVE ID : CVE-2021-0605**		
Use After Free	22-Jun-21	4.6	In drm_syncobj_handle_to_fd of drm_syncobj.c, there is a possible use after free due to incorrect refcounting. This could lead to local escalation of privilege with System execution privileges needed. User interaction is not needed for exploitation.Product: AndroidVersions: Android kernelAndroid ID: A-168034487 **CVE ID : CVE-2021-0606**	https://source.android.com/security/bulletin/pixel/2021-06-01	O-GOO-ANDR-020721/455
Improper Restriction of Operations within the Bounds of a Memory Buffer	22-Jun-21	4.6	In iaxxx_calc_i2s_div of iaxxx-codec.c, there is a possible hardware port write with user controlled data due to a missing bounds check. This could lead to local escalation of privilege with no additional execution privileges needed. User interaction is not needed for exploitation.Product: AndroidVersions: Android kernelAndroid ID: A-180950209 **CVE ID : CVE-2021-0607**	https://source.android.com/security/bulletin/pixel/2021-06-01	O-GOO-ANDR-020721/456
Externally Controlled Reference to a Resource in Another	22-Jun-21	4.6	In handleAppLaunch of AppLaunchActivity.java, there is a possible arbitrary activity launch due to a confused deputy. This could	https://source.android.com/security/bulletin/pixel/2021-06-	O-GOO-ANDR-020721/457

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Sphere			lead to local escalation of privilege with no additional execution privileges needed. User interaction is not needed for exploitation.Product: AndroidVersions: Android kernelAndroid ID: A-174870704 **CVE ID : CVE-2021-0608**	01	
HP					
hp-ux					
Improper Neutralization of Special Elements used in a Command ('Command Injection')	24-Jun-21	5	Db2 for Linux, UNIX and Windows (includes Db2 Connect Server) is vulnerable to a denial of service as the server terminates abnormally when executing a specially crafted SELECT statement. IBM X-Force ID: 200659. **CVE ID : CVE-2021-29703**	https://www.ibm.com/support/pages/node/6466371, https://exchange.xforce.ibmcloud.com/vulnerabilities/200659	O-HP-HP-U-020721/458
Huawei					
e3372_firmware					
Improper Preservation of Permissions	22-Jun-21	4.4	Huawei LTE USB Dongle products have an improper permission assignment vulnerability. An attacker can locally access and log in to a PC to induce a user to install a specially crafted application. After successfully exploiting this vulnerability, the attacker can perform unauthenticated operations. Affected product versions include:E3372 E3372h-153TCPU-	https://www.huawei.com/en/psirt/security-advisories/huawei-sa-20210602-01-permission-en	O-HUA-E337-020721/459

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			V200R002B333D01SP00C00. **CVE ID : CVE-2021-22382**		
e8372_firmware					
Improper Preservation of Permissions	22-Jun-21	4.4	Huawei LTE USB Dongle products have an improper permission assignment vulnerability. An attacker can locally access and log in to a PC to induce a user to install a specially crafted application. After successfully exploiting this vulnerability, the attacker can perform unauthenticated operations. Affected product versions include:E3372 E3372h-153TCPU-V200R002B333D01SP00C00. **CVE ID : CVE-2021-22382**	https://www.huawei.com/en/psirt/security-advisories/huawei-sa-20210602-01-permission-en	O-HUA-E837-020721/460
ecns280_firmware					
Incorrect Authorization	22-Jun-21	4.6	There is an improper authorization vulnerability in eCNS280 V100R005C00, V100R005C10 and eSE620X vESS V100R001C10SPC200, V100R001C20SPC200. A file access is not authorized correctly. Attacker with low access may launch privilege escalation in a specific scenario. This may compromise the normal service. **CVE ID : CVE-2021-22361**	https://www.huawei.com/en/psirt/security-advisories/huawei-sa-20210519-02-cgp-en	O-HUA-ECNS-020721/461
ecns280_td_firmware					
Allocation of Resources Without	22-Jun-21	5	There is a resource management error vulnerability in eCNS280_TD	https://www.huawei.com/en/psirt/	O-HUA-ECNS-020721/462

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Limits or Throttling			V100R005C10SPC650. An attacker needs to perform specific operations to exploit the vulnerability on the affected device. Due to improper resource management of the function, the vulnerability can be exploited to cause service abnormal on affected devices. **CVE ID : CVE-2021-22363**	security-advisories/huawei-sa-20210609-01-resource-en	
Concurrent Execution using Shared Resource with Improper Synchronization ('Race Condition')	22-Jun-21	3.5	There is a race condition vulnerability in eCNS280_TD V100R005C00 and V100R005C10. There is a timing window exists in which the database can be operated by another thread that is operating concurrently. Successful exploit may cause the affected device abnormal. **CVE ID : CVE-2021-22378**	https://www.huawei.com/en/psirt/security-advisories/huawei-sa-20210602-01-cgp-en	O-HUA-ECNS-020721/463
Out-of-bounds Read	22-Jun-21	6.8	There is an out-of-bounds read vulnerability in eCNS280_TD V100R005C10 and eSE620X vESS V100R001C10SPC200, V100R001C20SPC200, V200R001C00SPC300. The vulnerability is due to a message-handling function that contains an out-of-bounds read vulnerability. An attacker can exploit this vulnerability by sending a specific message to the target device, which could cause a Denial of Service (DoS).	https://www.huawei.com/en/psirt/security-advisories/huawei-sa-20210616-01-cgp-en	O-HUA-ECNS-020721/464

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2021-22383		
ese620x_vess_firmware					
Incorrect Authorization	22-Jun-21	4.6	There is an improper authorization vulnerability in eCNS280 V100R005C00, V100R005C10 and eSE620X vESS V100R001C10SPC200, V100R001C20SPC200. A file access is not authorized correctly. Attacker with low access may launch privilege escalation in a specific scenario. This may compromise the normal service. **CVE ID : CVE-2021-22361**	https://www.huawei.com/en/psirt/security-advisories/huawei-sa-20210519-02-cgp-en	O-HUA-ESE6-020721/465
Out-of-bounds Read	22-Jun-21	2.1	There is an out of bounds read vulnerability in eSE620X vESS V100R001C10SPC200, V100R001C20SPC200, V200R001C00SPC300. A local attacker can exploit this vulnerability by sending specific message to the target device. Due to insufficient validation of internal message, successful exploit may cause the process and the service abnormal. **CVE ID : CVE-2021-22365**	https://www.huawei.com/en/psirt/security-advisories/huawei-sa-20210526-02-outbounds-en	O-HUA-ESE6-020721/466
Out-of-bounds Read	22-Jun-21	4.9	There is an out-of-bounds read vulnerability in eSE620X vESS V100R001C10SPC200, V100R001C20SPC200, V200R001C00SPC300. The vulnerability is due to a function that handles an internal message contains an out-of-bounds read	https://www.huawei.com/en/psirt/security-advisories/huawei-sa-20210526-03-dos-en	O-HUA-ESE6-020721/467

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			vulnerability. An attacker could crafted messages between system process, successful exploit could cause Denial of Service (DoS). **CVE ID : CVE-2021-22366**		
Out-of-bounds Read	22-Jun-21	6.8	There is an out-of-bounds read vulnerability in eCNS280_TD V100R005C10 and eSE620X vESS V100R001C10SPC200, V100R001C20SPC200, V200R001C00SPC300. The vulnerability is due to a message-handling function that contains an out-of-bounds read vulnerability. An attacker can exploit this vulnerability by sending a specific message to the target device, which could cause a Denial of Service (DoS). **CVE ID : CVE-2021-22383**	https://www.huawei.com/en/psirt/security-advisories/huawei-sa-20210616-01-cgp-en	O-HUA-ESE6-020721/468
ips_module_firmware					
Improper Input Validation	22-Jun-21	4	There is an information leak vulnerability in Huawei products. A module does not deal with specific input sufficiently. High privilege attackers can exploit this vulnerability by performing some operations. This can lead to information leak. Affected product versions include: IPS Module versions V500R005C00, V500R005C10, V500R005C20; NGFW Module versions	https://www.huawei.com/en/psirt/security-advisories/huawei-sa-20210428-01-infomationleak-en	O-HUA-IPS_-020721/469

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			V500R005C00,V500R005C10 , V500R005C20; SeMG9811 versions V500R005C00; USG9500 versions V500R001C00, V500R001C20, V500R001C30, V500R001C50, V500R001C60, V500R001C80, V500R005C00, V500R005C10, V500R005C20. **CVE ID : CVE-2021-22342**		
ngfw_module_firmware					
Improper Input Validation	22-Jun-21	4	There is an information leak vulnerability in Huawei products. A module does not deal with specific input sufficiently. High privilege attackers can exploit this vulnerability by performing some operations. This can lead to information leak. Affected product versions include: IPS Module versions V500R005C00, V500R005C10, V500R005C20; NGFW Module versions V500R005C00,V500R005C10 , V500R005C20; SeMG9811 versions V500R005C00; USG9500 versions V500R001C00, V500R001C20, V500R001C30, V500R001C50, V500R001C60, V500R001C80,	https://www.huawei.com/en/psirt/security-advisories/huawei-sa-20210428-01-infomationleak-en	O-HUA-NGFW-020721/470

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			V500R005C00, V500R005C10, V500R005C20. **CVE ID : CVE-2021-22342**		
s12700_firmware					
Improper Input Validation	22-Jun-21	6.5	There is a command injection vulnerability in S12700 V200R019C00SPC500, S2700 V200R019C00SPC500, S5700 V200R019C00SPC500, S6700 V200R019C00SPC500 and S7700 V200R019C00SPC500. A module does not verify specific input sufficiently. Attackers can exploit this vulnerability by sending malicious parameters to inject command. This can compromise normal service. **CVE ID : CVE-2021-22377**	https://www.huawei.com/en/psirt/security-advisories/huawei-sa-20210602-01-cmdinj-en	O-HUA-S127-020721/471
s2700_firmware					
Improper Input Validation	22-Jun-21	6.5	There is a command injection vulnerability in S12700 V200R019C00SPC500, S2700 V200R019C00SPC500, S5700 V200R019C00SPC500, S6700 V200R019C00SPC500 and S7700 V200R019C00SPC500. A module does not verify specific input sufficiently. Attackers can exploit this vulnerability by sending malicious parameters to inject command. This can compromise normal service. **CVE ID : CVE-2021-22377**	https://www.huawei.com/en/psirt/security-advisories/huawei-sa-20210602-01-cmdinj-en	O-HUA-S270-020721/472
s5700_firmware					
Improper	22-Jun-21	6.5	There is a command injection	https://ww	O-HUA-S570-

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Input Validation			vulnerability in S12700 V200R019C00SPC500, S2700 V200R019C00SPC500, S5700 V200R019C00SPC500, S6700 V200R019C00SPC500 and S7700 V200R019C00SPC500. A module does not verify specific input sufficiently. Attackers can exploit this vulnerability by sending malicious parameters to inject command. This can compromise normal service. **CVE ID : CVE-2021-22377**	w.huawei.com/en/psirt/security-advisories/huawei-sa-20210602-01-cmdinj-en	020721/473
s6700_firmware					
Improper Input Validation	22-Jun-21	6.5	There is a command injection vulnerability in S12700 V200R019C00SPC500, S2700 V200R019C00SPC500, S5700 V200R019C00SPC500, S6700 V200R019C00SPC500 and S7700 V200R019C00SPC500. A module does not verify specific input sufficiently. Attackers can exploit this vulnerability by sending malicious parameters to inject command. This can compromise normal service. **CVE ID : CVE-2021-22377**	https://www.huawei.com/en/psirt/security-advisories/huawei-sa-20210602-01-cmdinj-en	O-HUA-S670-020721/474
s7700_firmware					
Improper Input Validation	22-Jun-21	6.5	There is a command injection vulnerability in S12700 V200R019C00SPC500, S2700 V200R019C00SPC500, S5700 V200R019C00SPC500, S6700 V200R019C00SPC500 and S7700 V200R019C00SPC500. A module does not verify	https://www.huawei.com/en/psirt/security-advisories/huawei-sa-20210602-01-cmdinj-en	O-HUA-S770-020721/475

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			specific input sufficiently. Attackers can exploit this vulnerability by sending malicious parameters to inject command. This can compromise normal service. **CVE ID : CVE-2021-22377**		
semg9811_firmware					
Improper Input Validation	22-Jun-21	4	There is an information leak vulnerability in Huawei products. A module does not deal with specific input sufficiently. High privilege attackers can exploit this vulnerability by performing some operations. This can lead to information leak. Affected product versions include: IPS Module versions V500R005C00, V500R005C10, V500R005C20; NGFW Module versions V500R005C00,V500R005C10, V500R005C20; SeMG9811 versions V500R005C00; USG9500 versions V500R001C00, V500R001C20, V500R001C30, V500R001C50, V500R001C60, V500R001C80, V500R005C00, V500R005C10, V500R005C20. **CVE ID : CVE-2021-22342**	https://www.huawei.com/en/psirt/security-advisories/huawei-sa-20210428-01-infomationleak-en	O-HUA-SEMG-020721/476
usg9500_firmware					
Improper	22-Jun-21	4	There is an information leak	https://ww	O-HUA-

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Input Validation			vulnerability in Huawei products. A module does not deal with specific input sufficiently. High privilege attackers can exploit this vulnerability by performing some operations. This can lead to information leak. Affected product versions include: IPS Module versions V500R005C00, V500R005C10, V500R005C20; NGFW Module versions V500R005C00,V500R005C10, V500R005C20; SeMG9811 versions V500R005C00; USG9500 versions V500R001C00, V500R001C20, V500R001C30, V500R001C50, V500R001C60, V500R001C80, V500R005C00, V500R005C10, V500R005C20. **CVE ID : CVE-2021-22342**	w.huawei.com/en/psirt/security-advisories/huawei-sa-20210428-01-infomationleak-en	USG9-020721/477
IBM					
aix					
Server-Side Request Forgery (SSRF)	16-Jun-21	4	IBM Security Identity Manager 6.0.2 is vulnerable to server-side request forgery (SSRF). By sending a specially crafted request, a remote authenticated attacker could exploit this vulnerability to obtain sensitive data. IBM X-Force ID: 197591.	https://exchange.xforce.ibmcloud.com/vulnerabilities/197591, https://www.ibm.com/support/pages/node/6464	O-IBM-AIX-020721/478

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2021-20483	081	
Exposure of Resource to Wrong Sphere	16-Jun-21	3.5	IBM Security Identity Manager 6.0.2 could allow an authenticated malicious user to change the passwords of other users in the Windows AD environment when IBM Security Identity Manager Windows Password Synch Plug-in is deployed and configured. IBM X-Force ID: 197789. **CVE ID : CVE-2021-20488**	https://exchange.xforce.ibmcloud.com/vulnerabilities/197789, https://www.ibm.com/support/pages/node/6464081	O-IBM-AIX-020721/479
Improper Neutralization of Special Elements in Output Used by a Downstream Component ('Injection')	16-Jun-21	5	Db2 for Linux, UNIX and Windows (includes Db2 Connect Server) 11.1.4 and 11.5.5 is vulnerable to a denial of service as the server terminates abnormally when executing a specially crafted SELECT statement. IBM X-Force ID: 200658. **CVE ID : CVE-2021-29702**	https://exchange.xforce.ibmcloud.com/vulnerabilities/200658, https://www.ibm.com/support/pages/node/6463985	O-IBM-AIX-020721/480
Improper Neutralization of Special Elements used in a Command ('Command Injection')	24-Jun-21	5	Db2 for Linux, UNIX and Windows (includes Db2 Connect Server) is vulnerable to a denial of service as the server terminates abnormally when executing a specially crafted SELECT statement. IBM X-Force ID: 200659. **CVE ID : CVE-2021-29703**	https://www.ibm.com/support/pages/node/6466371, https://exchange.xforce.ibmcloud.com/vulnerabilities/200659	O-IBM-AIX-020721/481
N/A	17-Jun-21	3.6	IBM AIX 7.1 could allow a non-privileged local user to exploit a vulnerability in the trace facility to expose sensitive information or cause a denial of service. IBM	https://exchange.xforce.ibmcloud.com/vulnerabilities/200663, https://ww	O-IBM-AIX-020721/482

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			X-Force ID: 200663. **CVE ID : CVE-2021-29706**	w.ibm.com/support/pages/node/6464369	
Linux					
linux_kernel					
Server-Side Request Forgery (SSRF)	16-Jun-21	4	IBM Security Identity Manager 6.0.2 is vulnerable to server-side request forgery (SSRF). By sending a specially crafted request, a remote authenticated attacker could exploit this vulnerability to obtain sensitive data. IBM X-Force ID: 197591. **CVE ID : CVE-2021-20483**	https://exchange.xforce.ibmcloud.com/vulnerabilities/197591, https://www.ibm.com/support/pages/node/6464081	O-LIN-LINU-020721/483
Exposure of Resource to Wrong Sphere	16-Jun-21	3.5	IBM Security Identity Manager 6.0.2 could allow an authenticated malicious user to change the passwords of other users in the Windows AD environment when IBM Security Identity Manager Windows Password Synch Plug-in is deployed and configured. IBM X-Force ID: 197789. **CVE ID : CVE-2021-20488**	https://exchange.xforce.ibmcloud.com/vulnerabilities/197789, https://www.ibm.com/support/pages/node/6464081	O-LIN-LINU-020721/484
Improper Neutralization of Special Elements in Output Used by a Downstream Component ('Injection')	16-Jun-21	5	Db2 for Linux, UNIX and Windows (includes Db2 Connect Server) 11.1.4 and 11.5.5 is vulnerable to a denial of service as the server terminates abnormally when executing a specially crafted SELECT statement. IBM X-Force ID: 200658. **CVE ID : CVE-2021-29702**	https://exchange.xforce.ibmcloud.com/vulnerabilities/200658, https://www.ibm.com/support/pages/node/6463985	O-LIN-LINU-020721/485

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Improper Neutralization of Special Elements used in a Command ('Command Injection')	24-Jun-21	5	Db2 for Linux, UNIX and Windows (includes Db2 Connect Server) is vulnerable to a denial of service as the server terminates abnormally when executing a specially crafted SELECT statement. IBM X-Force ID: 200659. **CVE ID : CVE-2021-29703**	https://www.ibm.com/support/pages/node/6466371, https://exchange.xforce.ibmcloud.com/vulnerabilities/200659	O-LIN-LINU-020721/486
Out-of-bounds Read	17-Jun-21	6.6	An Out-of-Bounds Read was discovered in arch/arm/mach-footbridge/personal-pci.c in the Linux kernel through 5.12.11 because of the lack of a check for a value that shouldn't be negative, e.g., access to element -2 of an array, aka CID-298a58e165e4. **CVE ID : CVE-2021-32078**	https://git.kernel.org/cgit/linux/kernel/git/torvalds/linux.git/commit/?id=298a58e165e447ccfaae35fe9f651f9d7e15166f, https://github.com/torvalds/linux/commit/298a58e165e447ccfaae35fe9f651f9d7e15166f	O-LIN-LINU-020721/487
Microsoft					
windows					
Server-Side Request Forgery (SSRF)	16-Jun-21	4	IBM Security Identity Manager 6.0.2 is vulnerable to server-side request forgery (SSRF). By sending a specially crafted request, a remote authenticated attacker could exploit this vulnerability to obtain sensitive data. IBM X-Force ID: 197591.	https://exchange.xforce.ibmcloud.com/vulnerabilities/197591, https://www.ibm.com/support/pages/node/6464	O-MIC-WIND-020721/488

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			CVE ID : CVE-2021-20483	081	
Exposure of Resource to Wrong Sphere	16-Jun-21	3.5	IBM Security Identity Manager 6.0.2 could allow an authenticated malicious user to change the passwords of other users in the Windows AD environment when IBM Security Identity Manager Windows Password Synch Plug-in is deployed and configured. IBM X-Force ID: 197789. **CVE ID : CVE-2021-20488**	https://exchange.xforce.ibmcloud.com/vulnerabilities/197789, https://www.ibm.com/support/pages/node/6464081	O-MIC-WIND-020721/489
N/A	18-Jun-21	4.9	VMware Tools for Windows (11.x.y prior to 11.3.0) contains a denial-of-service vulnerability in the VM3DMP driver. A malicious actor with local user privileges in the Windows guest operating system, where VMware Tools is installed, can trigger a PANIC in the VM3DMP driver leading to a denial-of-service condition in the Windows guest operating system. **CVE ID : CVE-2021-21997**	https://www.vmware.com/security/advisories/VMSA-2021-0011.html	O-MIC-WIND-020721/490
Improper Neutralization of Special Elements in Output Used by a Downstream Component ('Injection')	16-Jun-21	5	Db2 for Linux, UNIX and Windows (includes Db2 Connect Server) 11.1.4 and 11.5.5 is vulnerable to a denial of service as the server terminates abnormally when executing a specially crafted SELECT statement. IBM X-Force ID: 200658. **CVE ID : CVE-2021-29702**	https://exchange.xforce.ibmcloud.com/vulnerabilities/200658, https://www.ibm.com/support/pages/node/6463985	O-MIC-WIND-020721/491
Improper Neutralizatio	24-Jun-21	5	Db2 for Linux, UNIX and Windows (includes Db2	https://www.ibm.com/s	O-MIC-WIND-

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
n of Special Elements used in a Command ('Command Injection')			Connect Server) is vulnerable to a denial of service as the server terminates abnormally when executing a specially crafted SELECT statement. IBM X-Force ID: 200659. **CVE ID : CVE-2021-29703**	upport/pages/node/6466371, https://exchange.xforce.ibmcloud.com/vulnerabilities/200659	020721/492
Out-of-bounds Read	24-Jun-21	5.8	When drawing text onto a canvas with WebRender disabled, an out of bounds read could occur. *This bug only affects Firefox on Windows. Other operating systems are unaffected.*. This vulnerability affects Firefox < 89.0.1. **CVE ID : CVE-2021-29968**	https://bugzilla.mozilla.org/show_bug.cgi?id=1712047, https://www.mozilla.org/security/advisories/mfsa2021-27/	O-MIC-WIND-020721/493
Access of Resource Using Incompatible Type ('Type Confusion')	16-Jun-21	6.8	This vulnerability allows remote attackers to execute arbitrary code on affected installations of Foxit PhantomPDF 10.1.3.37598. User interaction is required to exploit this vulnerability in that the target must visit a malicious page or open a malicious file. The specific flaw exists within the handling of XFA templates. The issue results from the lack of proper validation of user-supplied data, which can result in a type confusion condition. An attacker can leverage this vulnerability to execute code in the context of the current process. Was ZDI-CAN-13531. **CVE ID : CVE-2021-31476**	https://www.foxit.com/support/security-bulletins.html	O-MIC-WIND-020721/494

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Unrestricted Upload of File with Dangerous Type	16-Jun-21	5.1	PHPMailer before 6.5.0 on Windows allows remote code execution if lang_path is untrusted data and has a UNC pathname. **CVE ID : CVE-2021-34551**	https://github.com/PHPMailer/PHPMailer/blob/master/SECURITY.md	O-MIC-WIND-020721/495
Uncontrolled Search Path Element	16-Jun-21	4.4	TeamViewer before 14.7.48644 on Windows loads untrusted DLLs in certain situations. **CVE ID : CVE-2021-34803**	https://community.teamviewer.com/English/discussion/111154/windows-v14-7-48644	O-MIC-WIND-020721/496
Moxa					
mgate_mb3180_firmware					
Uncontrolled Resource Consumption	18-Jun-21	5	An issue was discovered on MOXA Mgate MB3180 Version 2.1 Build 18113012. Attacker could send a huge amount of TCP SYN packet to make web service's resource exhausted. Then the web server is denial-of-service. **CVE ID : CVE-2021-33823**	https://www.moxa.com/en/products/industrial-edge-connectivity/protocol-gateways/modbus-tcp-gateways/mgate-mb3180-mb3280-mb3480-series	O-MOX-MGAT-020721/497
Uncontrolled Resource Consumption	18-Jun-21	5	An issue was discovered on MOXA Mgate MB3180 Version 2.1 Build 18113012. Attackers can use slowhttptest tool to send incomplete HTTP request, which could make server keep waiting for the packet to	https://www.moxa.com/en/products/industrial-edge-connectivity/protocol-gateways/m	O-MOX-MGAT-020721/498

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			finish the connection, until its resource exhausted. Then the web server is denial-of-service. **CVE ID : CVE-2021-33824**	odbus-tcp-gateways/mgate-mb3180-mb3280-mb3480-series	
Nvidia					
jetson_linux					
Integer Overflow or Wraparound	22-Jun-21	4.6	Trusty (the trusted OS produced by NVIDIA for Jetson devices) driver contains a vulnerability in the NVIDIA OTE protocol message parsing code where an integer overflow in a malloc() size calculation leads to a buffer overflow on the heap, which might result in information disclosure, escalation of privileges, and denial of service. **CVE ID : CVE-2021-34372**	https://nvidia.custhelp.com/app/answers/detail/a_id/5205	O-NVI-JETS-020721/499
Integer Overflow or Wraparound	21-Jun-21	4.6	Trusty TLK contains a vulnerability in the NVIDIA TLK kernel where an integer overflow in the calloc size calculation can cause the multiplication of count and size can overflow, which might lead to heap overflows. **CVE ID : CVE-2021-34386**	https://nvidia.custhelp.com/app/answers/detail/a_id/5205	O-NVI-JETS-020721/500
Incorrect Default Permissions	21-Jun-21	7.2	The ARM TrustZone Technology on which Trusty is based on contains a vulnerability in access permission settings where the portion of the DRAM reserved for TrustZone is	https://nvidia.custhelp.com/app/answers/detail/a_id/5205	O-NVI-JETS-020721/501

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			identity-mapped by TLK with read, write, and execute permissions, which gives write access to kernel code and data that is otherwise mapped read only. **CVE ID : CVE-2021-34387**		
Out-of-bounds Write	21-Jun-21	4.6	Bootloader contains a vulnerability in NVIDIA MB2 where a potential heap overflow might allow an attacker to control all the RAM after the heap block, leading to denial of service or code execution. **CVE ID : CVE-2021-34388**	https://nvidia.custhelp.com/app/answers/detail/a_id/5205	O-NVI-JETS-020721/502
Missing Release of Memory after Effective Lifetime	21-Jun-21	2.1	Trusty contains a vulnerability in NVIDIA OTE protocol message parsing code, which is present in all the TAs. An incorrect bounds check leads to a memory leak of a portion of the heap situated after a stream buffer. **CVE ID : CVE-2021-34389**	https://nvidia.custhelp.com/app/answers/detail/a_id/5205	O-NVI-JETS-020721/503
Integer Overflow or Wraparound	22-Jun-21	2.1	Trusty TLK contains a vulnerability in the NVIDIA TLK kernel function where a lack of checks allows the exploitation of an integer overflow on the size parameter of the tz_map_shared_mem function. **CVE ID : CVE-2021-34390**	https://nvidia.custhelp.com/app/answers/detail/a_id/5205	O-NVI-JETS-020721/504
Integer Overflow or Wraparound	22-Jun-21	4.9	Trusty TLK contains a vulnerability in the NVIDIA TLK kernelï¿½s tz_handle_trusted_app_smc	https://nvidia.custhelp.com/app/answers/detail/a_	O-NVI-JETS-020721/505

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			function where a lack of integer overflow checks on the req_off and param_ofs variables leads to memory corruption of critical kernel structures. **CVE ID : CVE-2021-34391**	id/5205	
Integer Overflow or Wraparound	22-Jun-21	2.1	Trusty TLK contains a vulnerability in the NVIDIA TLK kernel where an integer overflow in the tz_map_shared_mem function can bypass boundary checks, which might lead to denial of service. **CVE ID : CVE-2021-34392**	https://nvidia.custhelp.com/app/answers/detail/a_id/5205	O-NVI-JETS-020721/506
Deserialization of Untrusted Data	22-Jun-21	2.1	Trusty contains a vulnerability in TSEC TA which deserializes the incoming messages even though the TSEC TA does not expose any command. This vulnerability might allow an attacker to exploit the deserializer to impact code execution, causing information disclosure. **CVE ID : CVE-2021-34393**	https://nvidia.custhelp.com/app/answers/detail/a_id/5205	O-NVI-JETS-020721/507
Deserialization of Untrusted Data	22-Jun-21	4.6	Trusty contains a vulnerability in all TAs whose deserializer does not reject messages with multiple occurrences of the same parameter. The deserialization of untrusted data might allow an attacker to exploit the deserializer to impact code execution. **CVE ID : CVE-2021-34394**	https://nvidia.custhelp.com/app/answers/detail/a_id/5205	O-NVI-JETS-020721/508

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Incorrect Default Permissions	22-Jun-21	3.6	Trusty TLK contains a vulnerability in its access permission settings where it does not properly restrict access to a resource from a user with local privileges, which might lead to limited information disclosure and limited denial of service. **CVE ID : CVE-2021-34395**	https://nvidia.custhelp.com/app/answers/detail/a_id/5205	O-NVI-JETS-020721/509
Incorrect Authorization	22-Jun-21	2.1	Bootloader contains a vulnerability in access permission settings where unauthorized software may be able to overwrite NVIDIA MB2 code, which would result in limited denial of service. **CVE ID : CVE-2021-34396**	https://nvidia.custhelp.com/app/answers/detail/a_id/5205	O-NVI-JETS-020721/510
Out-of-bounds Write	22-Jun-21	2.1	Bootloader contains a vulnerability in NVIDIA MB2, which may cause free-the-wrong-heap, which may lead to limited denial of service. **CVE ID : CVE-2021-34397**	https://nvidia.custhelp.com/app/answers/detail/a_id/5205	O-NVI-JETS-020721/511
Oracle					
solaris					
Server-Side Request Forgery (SSRF)	16-Jun-21	4	IBM Security Identity Manager 6.0.2 is vulnerable to server-side request forgery (SSRF). By sending a specially crafted request, a remote authenticated attacker could exploit this vulnerability to obtain sensitive data. IBM X-Force ID: 197591. **CVE ID : CVE-2021-20483**	https://exchange.xforce.ibmcloud.com/vulnerabilities/197591, https://www.ibm.com/support/pages/node/6464081	O-ORA-SOLA-020721/512
Exposure of	16-Jun-21	3.5	IBM Security Identity	https://exch	O-ORA-

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Resource to Wrong Sphere			Manager 6.0.2 could allow an authenticated malicious user to change the passwords of other users in the Windows AD environment when IBM Security Identity Manager Windows Password Synch Plug-in is deployed and configured. IBM X-Force ID: 197789. **CVE ID : CVE-2021-20488**	ange.xforce.ibmcloud.com/vulnerabilities/197789, https://www.ibm.com/support/pages/node/6464081	SOLA-020721/513
Improper Neutralization of Special Elements used in a Command ('Command Injection')	24-Jun-21	5	Db2 for Linux, UNIX and Windows (includes Db2 Connect Server) is vulnerable to a denial of service as the server terminates abnormally when executing a specially crafted SELECT statement. IBM X-Force ID: 200659. **CVE ID : CVE-2021-29703**	https://www.ibm.com/support/pages/node/6466371, https://exchange.xforce.ibmcloud.com/vulnerabilities/200659	O-ORA-SOLA-020721/514
protectimus					
slim_nfc_70_firmware					
Improper Authentication	16-Jun-21	1.9	Protectimus SLIM NFC 70 10.01 devices allow a Time Traveler attack in which attackers can predict TOTP passwords in certain situations. The time value used by the device can be set independently from the used seed value for generating time-based one-time passwords, without authentication. Thus, an attacker with short-time physical access to a device can set the internal real-time clock (RTC) to the future,	N/A	O-PRO-SLIM-020721/515

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			generate one-time passwords, and reset the clock to the current time. This allows the generation of valid future time-based one-time passwords without having further access to the hardware token. **CVE ID : CVE-2021-32033**		
Qnap					
qts					
Insecure Storage of Sensitive Information	16-Jun-21	4	Insecure storage of sensitive information has been reported to affect QNAP NAS running myQNAPcloud Link. If exploited, this vulnerability allows remote attackers to read sensitive information by accessing the unrestricted storage mechanism. This issue affects: QNAP Systems Inc. myQNAPcloud Link versions prior to 2.2.21 on QTS 4.5.3; versions prior to 2.2.21 on QuTS hero h4.5.2; versions prior to 2.2.21 on QuTScloud c4.5.4. **CVE ID : CVE-2021-28815**	https://www.qnap.com/zh-tw/security-advisory/qsa-21-26	O-QNA-QTS-020721/516
qutscloud					
Insecure Storage of Sensitive Information	16-Jun-21	4	Insecure storage of sensitive information has been reported to affect QNAP NAS running myQNAPcloud Link. If exploited, this vulnerability allows remote attackers to read sensitive information by accessing the unrestricted storage mechanism. This issue affects: QNAP Systems	https://www.qnap.com/zh-tw/security-advisory/qsa-21-26	O-QNA-QUTS-020721/517

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			Inc. myQNAPcloud Link versions prior to 2.2.21 on QTS 4.5.3; versions prior to 2.2.21 on QuTS hero h4.5.2; versions prior to 2.2.21 on QuTScloud c4.5.4. **CVE ID : CVE-2021-28815**		
quts_hero					
Insecure Storage of Sensitive Information	16-Jun-21	4	Insecure storage of sensitive information has been reported to affect QNAP NAS running myQNAPcloud Link. If exploited, this vulnerability allows remote attackers to read sensitive information by accessing the unrestricted storage mechanism. This issue affects: QNAP Systems Inc. myQNAPcloud Link versions prior to 2.2.21 on QTS 4.5.3; versions prior to 2.2.21 on QuTS hero h4.5.2; versions prior to 2.2.21 on QuTScloud c4.5.4. **CVE ID : CVE-2021-28815**	https://www.qnap.com/zh-tw/security-advisory/qsa-21-26	O-QNA-QUTS-020721/518
Redhat					
linux					
Use of a Broken or Risky Cryptographic Algorithm	16-Jun-21	5	IBM Resilient SOAR V38.0 uses weaker than expected cryptographic algorithms that could allow an attacker to decrypt highly sensitive information. IBM X-Force ID: 199238. **CVE ID : CVE-2021-20566**	https://www.ibm.com/support/pages/node/6464043, https://exchange.xforce.ibmcloud.com/vulnerabilities/199238	O-RED-LINU-020721/519
Missing	16-Jun-21	2.1	IBM Resilient SOAR V38.0	https://ww	O-RED-LINU-

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Encryption of Sensitive Data			could allow a local privileged attacker to obtain sensitive information due to improper or nonexisting encryption.IBM X-Force ID: 199239. **CVE ID : CVE-2021-20567**	w.ibm.com/support/pages/node/6464039, https://exchange.xforce.ibmcloud.com/vulnerabilities/199239	020721/520
riot-os					
riot					
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	18-Jun-21	5	RIOT-OS 2021.01 before commit 85da504d2dc30188b89f44c3276fc5a25b31251f contains a buffer overflow which could allow attackers to obtain sensitive information. **CVE ID : CVE-2021-31660**	https://github.com/RIOT-OS/RIOT/commit/85da504d2dc30188b89f44c3276fc5a25b31251f	O-RIO-RIOT-020721/521
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	18-Jun-21	5	RIOT-OS 2021.01 before commit 609c9ada34da5546cffb632a98b7ba157c112658 contains a buffer overflow that could allow attackers to obtain sensitive information. **CVE ID : CVE-2021-31661**	https://github.com/RIOT-OS/RIOT/commit/609c9ada34da5546cffb632a98b7ba157c112658	O-RIO-RIOT-020721/522
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	18-Jun-21	5	RIOT-OS 2021.01 before commit 07f1254d8537497552e7dce80364aaead9266bbe contains a buffer overflow which could allow attackers to obtain sensitive information. **CVE ID : CVE-2021-31662**	https://github.com/RIOT-OS/RIOT/commit/07f1254d8537497552e7dce80364aaead9266bbe	O-RIO-RIOT-020721/523
Buffer Copy without Checking	18-Jun-21	5	RIOT-OS 2021.01 before commit bc59d60be60dfc0a05def57d	https://github.com/RIOT-OS/RIOT/co	O-RIO-RIOT-020721/524

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Size of Input ('Classic Buffer Overflow')			74985371e4f22d79 contains a buffer overflow which could allow attackers to obtain sensitive information. **CVE ID : CVE-2021-31663**	mmit/bc59d60be60dfc0a05def57d74985371e4f22d79	
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	18-Jun-21	5	RIOT-OS 2021.01 before commit 44741ff99f7a71df45420635b238b9c22093647a contains a buffer overflow which could allow attackers to obtain sensitive information. **CVE ID : CVE-2021-31664**	https://github.com/RIOT-OS/RIOT/commit/44741ff99f7a71df45420635b238b9c22093647a	O-RIO-RIOT-020721/525
serenityos					
serenityos					
Improper Limitation of a Pathname to a Restricted Directory ('Path Traversal')	18-Jun-21	7.5	SerenityOS before commit 3844e8569689dd476064a0759d704bc64fb3ca2c contains a directory traversal vulnerability in tar/unzip that may lead to command execution or privilege escalation. **CVE ID : CVE-2021-31272**	https://github.com/SerenityOS/serenity/pull/5713/commits/3844e8569689dd476064a0759d704bc64fb3ca2c, https://github.com/SerenityOS/serenity/pull/5713	O-SER-SERE-020721/526
Buffer Copy without Checking Size of Input ('Classic Buffer Overflow')	18-Jun-21	5	SerenityOS contains a buffer overflow in the set_range test in TestBitmap which could allow attackers to obtain sensitive information. **CVE ID : CVE-2021-33185**	https://github.com/SerenityOS/serenity/issues/7073	O-SER-SERE-020721/527
Out-of-bounds Write	18-Jun-21	5	SerenityOS in test-crypto.cpp contains a stack buffer overflow which could allow	https://github.com/SerenityOS/serenit	O-SER-SERE-020721/528

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			attackers to obtain sensitive information. **CVE ID : CVE-2021-33186**	y/issues/7072	
sing4g					
4gee_router_hh70vb_firmware					
Uncontrolled Resource Consumption	18-Jun-21	5	An issue was discovered on 4GEE ROUTER HH70VB Version HH70_E1_02.00_22. Attackers can use slowhttptest tool to send incomplete HTTP request, which could make server keep waiting for the packet to finish the connection, until its resource exhausted. Then the web server is denial-of-service. **CVE ID : CVE-2021-33822**	https://www.sing4g.com/product-page/4gee-router-hh70vb-4g-300mbps-2lan-32wifi	O-SIN-4GEE-020721/529
Sonicwall					
sonicos					
Exposure of Sensitive Information to an Unauthorized Actor	23-Jun-21	5	A vulnerability in SonicOS where the HTTP server response leaks partial memory by sending a crafted HTTP request, this can potentially lead to an internal sensitive data disclosure vulnerability. **CVE ID : CVE-2021-20019**	https://psirt.global.sonicwall.com/vuln-detail/SNWLID-2021-0006	O-SON-SONI-020721/530
sonicosv					
Exposure of Sensitive Information to an Unauthorized Actor	23-Jun-21	5	A vulnerability in SonicOS where the HTTP server response leaks partial memory by sending a crafted HTTP request, this can potentially lead to an internal sensitive data disclosure	https://psirt.global.sonicwall.com/vuln-detail/SNWLID-2021-0006	O-SON-SONI-020721/531

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
			vulnerability. **CVE ID : CVE-2021-20019**		
Synology					
diskstation_manager_unified_controller					
Use After Free	23-Jun-21	7.5	Use after free vulnerability in file transfer protocol component in Synology DiskStation Manager (DSM) before 6.2.3-25426-3 allows remote attackers to execute arbitrary code via unspecified vectors. **CVE ID : CVE-2021-27649**	https://www.synology.com/security/advisory/Synology_SA_20_26	O-SYN-DISK-020721/532
Improper Neutralization of Special Elements in Output Used by a Downstream Component ('Injection')	23-Jun-21	5	Improper neutralization of special elements in output used by a downstream component ('Injection') vulnerability in Security Advisor report management component in Synology DiskStation Manager (DSM) before 6.2.3-25426-3 allows remote attackers to read arbitrary files via unspecified vectors. **CVE ID : CVE-2021-29084**	https://www.synology.com/security/advisory/Synology_SA_20_26	O-SYN-DISK-020721/533
Improper Neutralization of Special Elements in Output Used by a Downstream Component ('Injection')	23-Jun-21	5	Improper neutralization of special elements in output used by a downstream component ('Injection') vulnerability in file sharing management component in Synology DiskStation Manager (DSM) before 6.2.3-25426-3 allows remote attackers to read arbitrary files via unspecified vectors. **CVE ID : CVE-2021-29085**	https://www.synology.com/security/advisory/Synology_SA_20_26	O-SYN-DISK-020721/534

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Exposure of Sensitive Information to an Unauthorized Actor	23-Jun-21	5	Exposure of sensitive information to an unauthorized actor vulnerability in webapi component in Synology DiskStation Manager (DSM) before 6.2.3-25426-3 allows remote attackers to obtain sensitive information via unspecified vectors. **CVE ID : CVE-2021-29086**	https://www.synology.com/security/advisory/Synology_SA_20_26	O-SYN-DISK-020721/535
Improper Limitation of a Pathname to a Restricted Directory ('Path Traversal')	23-Jun-21	5	Improper limitation of a pathname to a restricted directory ('Path Traversal') vulnerability in webapi component in Synology DiskStation Manager (DSM) before 6.2.3-25426-3 allows remote attackers to write arbitrary files via unspecified vectors. **CVE ID : CVE-2021-29087**	https://www.synology.com/security/advisory/Synology_SA_20_26	O-SYN-DISK-020721/536
Trendnet					
tw100-s4w1ca_firmware					
Cross-Site Request Forgery (CSRF)	17-Jun-21	6.8	In TrendNet TW100-S4W1CA 2.3.32, due to a lack of proper session controls, a threat actor could make unauthorized changes to an affected router via a specially crafted web page. If an authenticated user were to interact with a malicious web page it could allow for a complete takeover of the router. **CVE ID : CVE-2021-32424**	N/A	O-TRE-TW10-020721/537
Improper	17-Jun-21	4.3	In TrendNet TW100-S4W1CA	N/A	O-TRE-

Weakness	Publish Date	CVSS	Description & CVE ID	Patch	NCIIPC ID
Neutralization of Input During Web Page Generation ('Cross-site Scripting')			2.3.32, it is possible to inject arbitrary JavaScript into the router's web interface via the "echo" command. **CVE ID : CVE-2021-32426**		TW10-020721/538
ui					
camera_g3_flex_firmware					
Uncontrolled Resource Consumption	18-Jun-21	5	An issue was discovered in UniFi Protect G3 FLEX Camera Version UVC.v4.30.0.67. Attackers can use slowhttptest tool to send incomplete HTTP request, which could make server keep waiting for the packet to finish the connection, until its resource exhausted. Then the web server is denial-of-service. **CVE ID : CVE-2021-33818**	https://store.ui.com/collections/unifi-protect-cameras/products/unifi-video-g3-flex-camera	O-UI-CAME-020721/539
Uncontrolled Resource Consumption	18-Jun-21	5	An issue was discovered in UniFi Protect G3 FLEX Camera Version UVC.v4.30.0.67.Attacker could send a huge amount of TCP SYN packet to make web service's resource exhausted. Then the web server is denial-of-service. **CVE ID : CVE-2021-33820**	https://store.ui.com/collections/unifi-protect-cameras/products/unifi-video-g3-flex-camera	O-UI-CAME-020721/540