SingCERT
Singapore Cyber Emergency Response Team

Security Bulletin 08 December 2021

SingCERT's Security Bulletin summarises the list of vulnerabilities collated from the National Institute of Standards and Technology (NIST)'s National Vulnerability Database (NVD) in the past week.

The vulnerabilities are tabled based on severity, in accordance to their CVSSv3 base scores:

Critical	vulnerabilities with a base score of 9.0 to 10.0
High	vulnerabilities with a base score of 7.0 to 8.9
Medium	vulnerabilities with a base score of 4.0 to 6.9
Low	vulnerabilities with a base score of 0.1 to 3.9
None	vulnerabilities with a base score of 0.0

For those vulnerabilities without assigned CVSS scores, please visit NVD for the updated CVSS vulnerability entries.

CRITICAL VULNERABILITIES

CVE Number	Description	Base Score	Reference
CVE-2021-43936	The software allows the attacker to upload or transfer files of dangerous types to the WebHMI portal, that may be automatically processed within the product's environment or lead to arbitrary code execution.	10.0	More Details
CVE-2021-26334	The AMDPowerProfiler.sys driver of AMD µProf tool may allow lower privileged users to access MSRs in kernel which may lead to privilege escalation and ring-0 code execution by the lower privileged user.	9.9	More Details
CVE-2021-24943	The Registrations for the Events Calendar WordPress plugin before 2.7.6 does not sanitise and escape the event_id in the rtec_send_unregister_link AJAX action (available to both unauthenticated and authenticated users) before using it in a SQL statement, leading to an unauthenticated SQL injection.	9.8	More Details

CVE Number	Description	Base Score	Reference
CVE-2021-44681	An issue (5 of 6) was discovered in Veritas Enterprise Vault through 14.1.2. On start-up, the Enterprise Vault application starts several services that listen on random .NET Remoting TCP ports for possible commands from client applications. These TCP services can be exploited due to deserialization behavior that is inherent to the .NET Remoting service. A malicious attacker can exploit both TCP remoting services and local IPC services on the Enterprise Vault Server. This vulnerability is mitigated by properly configuring the servers and firewall as described in the vendor's security alert for this vulnerability (VTS21-003, ZDI-CAN-14080).	9.8	More Details
CVE-2021-43044	An issue was discovered in Kaseya Unitrends Backup Appliance before 10.5.5. The SNMP daemon was configured with a weak default community.	9.8	More Details
CVE-2021-24866	The WP Data Access WordPress plugin before 5.0.0 does not properly sanitise and escape the backup_date parameter before using it a SQL statement, leading to a SQL injection issue and could allow arbitrary table deletion	9.8	More Details
CVE-2021-24931	The Secure Copy Content Protection and Content Locking WordPress plugin before 2.8.2 does not escape the sccp_id parameter of the ays_sccp_results_export_file AJAX action (available to both unauthenticated and authenticated users) before using it in a SQL statement, leading to an SQL injection.	9.8	More Details
CVE-2021-43931	The authentication algorithm of the WebHMI portal is sound, but the implemented mechanism can be bypassed as the result of a separate weakness that is primary to the authentication error.	9.8	More Details
CVE-2021-36564	ThinkPHP v6.0.8 was discovered to contain a deserialization vulnerability via the component vendor\league\flysystem-cached-adapter\src\Storage\Adapter.php.	9.8	More Details
CVE-2021-36567	ThinkPHP v6.0.8 was discovered to contain a deserialization vulnerability via the component League\Flysystem\Cached\Storage\AbstractCache.	9.8	More Details
CVE-2021-40091	An SSRF issue was discovered in SquaredUp for SCOM 5.2.1.6654.	9.8	More Details
CVE-2021-31632	b2evolution CMS v7.2.3 was discovered to contain a SQL injection vulnerability via the parameter cfqueryparam in the User login section. This vulnerability allows attackers to execute arbitrary code via a crafted input.	9.8	More Details

CVE Number	Description	Base Score	Reference
CVE-2021-44677	An issue (1 of 6) was discovered in Veritas Enterprise Vault through 14.1.2. On start-up, the Enterprise Vault application starts several services that listen on random .NET Remoting TCP ports for possible commands from client applications. These TCP services can be exploited due to deserialization behavior that is inherent to the .NET Remoting service. A malicious attacker can exploit both TCP remoting services and local IPC services on the Enterprise Vault Server. This vulnerability is mitigated by properly configuring the servers and firewall as described in the vendor's security alert for this vulnerability (VTS21-003, ZDI-CAN-14078).	9.8	More Details
CVE-2021-44678	An issue (2 of 6) was discovered in Veritas Enterprise Vault through 14.1.2. On start-up, the Enterprise Vault application starts several services that listen on random .NET Remoting TCP ports for possible commands from client applications. These TCP services can be exploited due to deserialization behavior that is inherent to the .NET Remoting service. A malicious attacker can exploit both TCP remoting services and local IPC services on the Enterprise Vault Server. This vulnerability is mitigated by properly configuring the servers and firewall as described in the vendor's security alert for this vulnerability (VTS21-003, ZDI-CAN-14076).	9.8	More Details
CVE-2021-44679	An issue (3 of 6) was discovered in Veritas Enterprise Vault through 14.1.2. On start-up, the Enterprise Vault application starts several services that listen on random .NET Remoting TCP ports for possible commands from client applications. These TCP services can be exploited due to deserialization behavior that is inherent to the .NET Remoting service. A malicious attacker can exploit both TCP remoting services and local IPC services on the Enterprise Vault Server. This vulnerability is mitigated by properly configuring the servers and firewall as described in the vendor's security alert for this vulnerability (VTS21-003, ZDI-CAN-14074).	9.8	More Details
CVE-2021-44680	An issue (4 of 6) was discovered in Veritas Enterprise Vault through 14.1.2. On start-up, the Enterprise Vault application starts several services that listen on random .NET Remoting TCP ports for possible commands from client applications. These TCP services can be exploited due to deserialization behavior that is inherent to the .NET Remoting service. A malicious attacker can exploit both TCP remoting services and local IPC services on the Enterprise Vault Server. This vulnerability is mitigated by properly configuring the servers and firewall as described in the vendor's security alert for this vulnerability (VTS21-003, ZDI-CAN-14075).	9.8	More Details

CVE Number	Description	Base Score	Reference
CVE-2021-44682	An issue (6 of 6) was discovered in Veritas Enterprise Vault through 14.1.2. On start-up, the Enterprise Vault application starts several services that listen on random .NET Remoting TCP ports for possible commands from client applications. These TCP services can be exploited due to deserialization behavior that is inherent to the .NET Remoting service. A malicious attacker can exploit both TCP remoting services and local IPC services on the Enterprise Vault Server. This vulnerability is mitigated by properly configuring the servers and firewall as described in the vendor's security alert for this vulnerability (VTS21-003, ZDI-CAN-14079).	9.8	More Details
CVE-2021-43036	An issue was discovered in Kaseya Unitrends Backup Appliance before 10.5.5. The password for the PostgreSQL wguest account is weak.	9.8	More Details
CVE-2021-44684	naholyr github-todos 3.1.0 is vulnerable to command injection. The range argument for the _hook subcommand is concatenated without any validation, and is directly used by the exec function.	9.8	More Details
CVE-2021-44685	Git-it through 4.4.0 allows OS command injection at the Branches Aren't Just For Birds challenge step. During the verification process, it attempts to run the reflog command followed by the current branch name (which is not sanitized for execution).	9.8	More Details
CVE-2021-29114	A SQL injection vulnerability in feature services provided by Esri ArcGIS Server 10.9 and below allows a remote, unauthenticated attacker to impact the confidentiality, integrity and availability of targeted services via specifically crafted queries.	9.8	More Details
CVE-2021-42127	A deserialization of untrusted data vulnerability exists in Ivanti Avalanche before 6.3.3 using Inforail Service allows arbitrary code execution via Data Repository Service.	9.8	More Details
CVE-2021-42128	An exposed dangerous function vulnerability exists in Ivanti Avalanche before 6.3.3 using inforail Service allows Privilege Escalation via Enterprise Server Service.	9.8	More Details
CVE-2021-37059	There is a Weaknesses Introduced During Design	9.8	More Details
CVE-2021-37063	There is a Cryptographic Issues vulnerability in Huawei Smartphone.Successful exploitation of this vulnerability may lead to read and delete images of Harmony devices.	9.8	More Details
CVE-2021-37084	There is a Improper Input Validation vulnerability in Huawei Smartphone.Successful exploitation of this vulnerability may lead to malicious invoking other functions of the Smart Assistant through text messages.	9.8	More Details

CVE Number	Description	Base Score	Reference
CVE-2021-37095	There is a Integer Overflow or Wraparound vulnerability in Huawei Smartphone.Successful exploitation of this vulnerability may lead to remote denial of service and potential remote code execution.	9.8	More Details
CVE-2021-24041	A missing bounds check in image blurring code prior to WhatsApp for Android v2.21.22.7 and WhatsApp Business for Android v2.21.22.7 could have allowed an out-of-bounds write if a user sent a malicious image.	9.8	More Details
CVE-2021-40859	Backdoors were discovered in Auerswald COMpact 5500R 7.8A and 8.0B devices, that allow attackers with access to the web based management application full administrative access to the device.	9.8	More Details
CVE-2021-41716	Maharashtra State Electricity Board Mahavitara Android Application 8.20 and prior is vulnerable to remote account takeover due to OTP fixation vulnerability in password rest function	9.8	More Details
CVE-2021-43042	An issue was discovered in Kaseya Unitrends Backup Appliance before 10.5.5. A buffer overflow existed in the vaultServer component. This was exploitable by a remote unauthenticated attacker.	9.8	More Details
CVE-2021-38759	Raspberry Pi OS through 5.10 has the raspberry default password for the pi account. If not changed, attackers can gain administrator privileges.	9.8	More Details
CVE-2021-43035	An issue was discovered in Kaseya Unitrends Backup Appliance before 10.5.5. Two unauthenticated SQL injection vulnerabilities were discovered, allowing arbitrary SQL queries to be injected and executed under the postgres superuser account. Remote code execution was possible, leading to full access to the postgres user account.	9.8	More Details
CVE-2021-43679	ecshop v2.7.3 is affected by a SQL injection vulnerability in shopex\ecshop\upload\api\client\api.php.	9.8	More Details
CVE-2021-44280	attendance management system 1.0 is affected by a SQL injection vulnerability in admin/incFunctions.php through the makeSafe function.	9.8	More Details
CVE-2021-43685	libretime hv3.0.0-alpha.10 is affected by a path manipulation vulnerability in /blob/master/legacy/application/modules/rest/controllers/ShowImageController.php through the rename function.	9.8	More Details
CVE-2021-43451	SQL Injection vulnerability exists in PHPGURUKUL Employee Record Management System 1.2 via the Email POST parameter in /forgetpassword.php.	9.8	More Details

CVE Number	Description	Base Score	Reference
CVE-2021-33265	D-Link DIR-809 devices with firmware through DIR-809Ax_FW1.12WWB03_20190410 were discovered to contain a stack buffer overflow vulnerability in the function FUN_80046eb4 in /formSetPortTr. This vulnerability is triggered via a crafted POST request.	9.8	More Details
CVE-2021-33266	D-Link DIR-809 devices with firmware through DIR-809Ax_FW1.12WWB03_20190410 were discovered to contain a stack buffer overflow vulnerability in the function FUN_8004776c in /formVirtualApp. This vulnerability is triggered via a crafted POST request.	9.8	More Details
CVE-2021-33267	D-Link DIR-809 devices with firmware through DIR-809Ax_FW1.12WWB03_20190410 were discovered to contain a stack buffer overflow vulnerability in the function FUN_80034d60 in /formStaticDHCP. This vulnerability is triggered via a crafted POST request.	9.8	More Details
CVE-2021-33268	D-Link DIR-809 devices with firmware through DIR-809Ax_FW1.12WWB03_20190410 were discovered to contain a stack buffer overflow vulnerability in the function sub_8003183C in /fromLogin. This vulnerability is triggered via a crafted POST request.	9.8	More Details
CVE-2021-33269	D-Link DIR-809 devices with firmware through DIR-809Ax_FW1.12WWB03_20190410 were discovered to contain a stack buffer overflow vulnerability in the function FUN_8004776c in /formVirtualServ. This vulnerability is triggered via a crafted POST request.	9.8	More Details
CVE-2021-43033	An issue was discovered in Kaseya Unitrends Backup Appliance before 10.5.5. Multiple functions in the bpserverd daemon were vulnerable to arbitrary remote code execution as root. The vulnerability was caused by untrusted input (received by the server) being passed to system calls.	9.8	More Details
CVE-2021-33271	D-Link DIR-809 devices with firmware through DIR-809Ax_FW1.12WWB03_20190410 were discovered to contain a stack buffer overflow vulnerability in the function sub_80046EB4 in /formSetPortTr. This vulnerability is triggered via a crafted POST request.	9.8	More Details
CVE-2021-33274	D-Link DIR-809 devices with firmware through DIR-809Ax_FW1.12WWB03_20190410 were discovered to contain a stack buffer overflow vulnerability in the function FUN_80040af8 in /formWlanSetup. This vulnerability is triggered via a crafted POST request.	9.8	More Details
CVE-2021-26777	Buffer overflow vulnerability in function SetFirewall in index.cgi in CIRCUTOR COMPACT DC-S BASIC smart metering concentrator Firwmare version CIR_CDC_v1.2.17, allows attackers to execute arbitrary code.	9.8	More Details
CVE-2021-33270	D-Link DIR-809 devices with firmware through DIR-809Ax_FW1.12WWB03_20190410 were discovered to contain a stack buffer overflow vulnerability in the function FUN_800462c4 in /formAdvFirewall. This vulnerability is triggered via a crafted POST request.	9.8	More Details

CVE Number	Description	Base Score	Reference
CVE-2021-44352	A Stack-based Buffer Overflow vulnerability exists in the Tenda AC15 V15.03.05.18_multi device via the list parameter in a post request in goform/SetIpMacBind.	9.8	More Details
CVE-2021-44347	SQL Injection vulnerability exists in TuziCMS v2.0.6 in App\Manage\Controller\GuestbookController.class.php.	9.8	More Details
CVE-2021-44348	SQL Injection vulnerability exists in TuziCMS v2.0.6 via the id parameer in App\Manage\Controller\AdvertController.class.php.	9.8	More Details
CVE-2021-35346	tsMuxer v2.6.16 was discovered to contain a heap-based buffer overflow via the function HevcSpsUnit::short_term_ref_pic_set(int) in hevc.cpp.	9.8	More Details
CVE-2021-35344	tsMuxer v2.6.16 was discovered to contain a heap-based buffer overflow via the function BitStreamReader::getCurVal in bitStream.h.	9.8	More Details
CVE-2021-35414	Chamilo LMS v1.11.x was discovered to contain a SQL injection via the doc parameter in main/plagiarism/compilatio/upload.php.	9.8	More Details
CVE-2021-44349	SQL Injection vulnerability exists in TuziCMS v2.0.6 via the id parameter in App\Manage\Controller\DownloadController.class.php.	9.8	More Details
CVE-2021-43676	matyhtf framework v3.0.5 is affected by a path manipulation vulnerability in Smarty.class.php.	9.8	More Details
CVE-2021-28237	LibreDWG v0.12.3 was discovered to contain a heap-buffer overflow via decode_preR13.	9.8	More Details
CVE-2021-44278	Librenms 21.11.0 is affected by a path manipulation vulnerability in includes/html/pages/device/showconfig.inc.php.	9.8	More Details
CVE-2021-43674	ThinkUp 2.0-beta.10 is affected by a path manipulation vulnerability in Smarty.class.php. NOTE: This vulnerability only affects products that are no longer supported by the maintainer	9.8	More Details
CVE-2021-3994	django-helpdesk is vulnerable to Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	9.6	More Details

CVE Number	Description	Base Score	Reference
CVE-2015-20105	The ClickBank Affiliate Ads WordPress plugin through 1.20 does not have CSRF check when saving its settings, allowing attacker to make logged in admin change them via a CSRF attack. Furthermore, due to the lack of escaping when they are outputting, it could also lead to Stored Cross-Site Scripting issues	9.6	More Details
CVE-2021-37079	There is a Improper Input Validation vulnerability in Huawei Smartphone.Successful exploitation of this vulnerability may lead to delete arbitrary file by system_app permission.	9.1	More Details
CVE-2021-37099	There is a Path Traversal vulnerability in Huawei Smartphone.Successful exploitation of this vulnerability may lead to delete any file.	9.1	More Details
CVE-2021-37088	There is a Path Traversal vulnerability in Huawei Smartphone.Successful exploitation of this vulnerability may lead to attackers can write any content to any file.	9.1	More Details
CVE-2021-37087	There is a Path Traversal vulnerability in Huawei Smartphone.Successful exploitation of this vulnerability may lead to attackers can create arbitrary file.	9.1	More Details
CVE-2020-29177	Z-BlogPHP v1.6.1.2100 was discovered to contain an arbitrary file deletion vulnerability via \app_del.php.	9.1	More Details
CVE-2021-37064	There is a Improper Limitation of a Pathname to a Restricted Directory vulnerability in Huawei Smartphone.Successful exploitation of this vulnerability may lead to arbitrary file created.	9.1	More Details
CVE-2021-37065	There is a Integer Overflow or Wraparound vulnerability in Huawei Smartphone.Successful exploitation of this vulnerability may lead to Confidentiality or Availability impacted.	9.1	More Details
CVE-2021-37041	There is an Improper verification vulnerability in Huawei Smartphone.Successful exploitation of this vulnerability may cause out-of-bounds read.	9.1	More Details
CVE-2021-37021	There is a Stack-based Buffer Overflow vulnerability in Huawei Smartphone.Successful exploitation of this vulnerability may lead to Out-of-bounds read.	9.1	More Details
CVE-2021-37020	There is a Stack-based Buffer Overflow vulnerability in Huawei Smartphone.Successful exploitation of this vulnerability may lead to Out-of-bounds read.	9.1	More Details
CVE-2021-37011	There is a Stack-based Buffer Overflow vulnerability in Huawei Smartphone.Successful exploitation of this vulnerability may lead to Out-of-bounds read.	9.1	More Details

CVE Number	Description	Base Score	Reference
CVE-2021-37042	There is an Improper verification vulnerability in Huawei Smartphone.Successful exploitation of this vulnerability may cause out-of-bounds read.	9.1	More Details
CVE-2021-37062	There is a Improper Validation of Array Index vulnerability in Huawei Smartphone.Successful exploitation of this vulnerability may lead to memory overflow and information leakage.	9.1	More Details
CVE-2021-40333	Weak Password Requirements vulnerability in Hitachi Energy FOX61x, XCM20 allows an attacker to gain unauthorized access to the Data Communication Network (DCN) routing configuration. This issue affects: Hitachi Energy FOX61x versions prior to R15A. Hitachi Energy XCM20 versions prior to R15A.	9.0	More Details
CVE-2021-3985	kimai2 is vulnerable to Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	9.0	More Details

OTHER VULNERABILITIES

CVE Number	Description	Base Score	Reference
CVE-2021-40809	An issue was discovered in Jamf Pro before 10.32.0, aka PI-009921. An account can be granted incorrect privileges in response to authentication that uses specific sign-on workflows.	8.8	More Details
CVE-2021-43638	Amazon Amazon WorkSpaces agent is affected by Integer Overflow. IOCTL Handler 0x22001B in the Amazon WorkSpaces agent below v1.0.1.1537 allow local attackers to execute arbitrary code in kernel mode or cause a denial of service (memory corruption and OS crash) via specially crafted I/O Request Packet.	8.8	More Details
CVE-2021-42980	NoMachine Cloud Server is affected by Buffer Overflow. IOCTL Handler 0x22001B in the NoMachine Cloud Server above 4.0.346 and below 7.7.4 allow local attackers to execute arbitrary code in kernel mode or cause a denial of service (memory corruption and OS crash) via specially crafted I/O Request Packet.	8.8	More Details
CVE-2021-42983	NoMachine Enterprise Client is affected by Buffer Overflow. IOCTL Handler 0x22001B in the NoMachine Enterprise Client above 4.0.346 and below 7.7.4 allow local attackers to execute arbitrary code in kernel mode or cause a denial of service (memory corruption and OS crash) via specially crafted I/O Request Packet.	8.8	More Details

CVE Number	Description	Base Score	Reference
CVE-2021-42986	NoMachine Enterprise Client is affected by Integer Overflow. IOCTL Handler 0x22001B in the NoMachine Enterprise Client above 4.0.346 and below 7.7.4 allow local attackers to execute arbitrary code in kernel mode or cause a denial of service (memory corruption and OS crash) via specially crafted I/O Request Packet.	8.8	More Details
CVE-2021-42987	Eltima USB Network Gate is affected by Integer Overflow. IOCTL Handler 0x22001B in the USB Network Gate above 7.0.1370 below 9.2.2420 allow local attackers to execute arbitrary code in kernel mode or cause a denial of service (memory corruption and OS crash) via specially crafted I/O Request Packet.	8.8	More Details
CVE-2021-42988	Eltima USB Network Gate is affected by Buffer Overflow. IOCTL Handler 0x22001B in the USB Network Gate above 7.0.1370 below 9.2.2420 allow local attackers to execute arbitrary code in kernel mode or cause a denial of service (memory corruption and OS crash) via specially crafted I/O Request Packet.	8.8	More Details
CVE-2021-42990	FlexiHub For Windows is affected by Buffer Overflow. IOCTL Handler 0x22001B in the FlexiHub For Windows above 2.0.4340 below 5.3.14268 allows local attackers to execute arbitrary code in kernel mode or cause a denial of service (memory corruption and OS crash) via specially crafted I/O Request Packet.	8.8	More Details
CVE-2021-42993	FlexiHub For Windows is affected by Integer Overflow. IOCTL Handler 0x22001B in the FlexiHub For Windows above 2.0.4340 below 5.3.14268 allow local attackers to execute arbitrary code in kernel mode or cause a denial of service (memory corruption and OS crash) via specially crafted I/O Request Packet.	8.8	More Details
CVE-2021-43038	An issue was discovered in Kaseya Unitrends Backup Appliance before 10.5.5. The wguest account could execute commands by injecting into PostgreSQL trigger functions. This allowed privilege escalation from the wguest user to the postgres user.	8.8	More Details
CVE-2021-42994	Donglify is affected by Buffer Overflow. IOCTL Handler 0x22001B in the Donglify above 1.0.12309 below 1.7.14110 allow local attackers to execute arbitrary code in kernel mode or cause a denial of service (memory corruption and OS crash) via specially crafted I/O Request Packet.	8.8	More Details
CVE-2021-42996	Donglify is affected by Integer Overflow. IOCTL Handler 0x22001B in the Donglify above 1.0.12309 below 1.7.14110 allow local attackers to execute arbitrary code in kernel mode or cause a denial of service (memory corruption and OS crash) via specially crafted I/O Request Packet.	8.8	More Details
CVE-2021-43000	Amzetta zPortal Windows zClient is affected by Buffer Overflow. IOCTL Handler 0x22001B in the Amzetta zPortal Windows zClient <= v3.2.8180.148 allow local attackers to execute arbitrary code in kernel mode or cause a denial of service (memory corruption and OS crash) via specially crafted I/O Request Packet.	8.8	More Details

CVE Number	Description	Base Score	Reference
CVE-2021-43002	Amzetta zPortal DVM Tools is affected by Buffer Overflow. IOCTL Handler 0x22001B in the Amzetta zPortal DVM Tools <= v3.3.148.148 allow local attackers to execute arbitrary code in kernel mode or cause a denial of service (memory corruption and OS crash) via specially crafted I/O Request Packet.	8.8	More Details
CVE-2021-43137	Cross-Site Scripting (XSS) and Cross-Site Request Forgery (CSRF) vulnerability exits in hostel management system 2.1 via the name field in my-profile.php. Chaining to this both vulnerabilities leads to account takeover.	8.8	More Details
CVE-2021-43003	Amzetta zPortal Windows zClient is affected by Integer Overflow. IOCTL Handler 0x22001B in the Amzetta zPortal Windows zClient <= v3.2.8180.148 allow local attackers to execute arbitrary code in kernel mode or cause a denial of service (memory corruption and OS crash) via specially crafted I/O Request Packet.	8.8	More Details
CVE-2021-43006	AmZetta Amzetta zPortal DVM Tools is affected by Integer Overflow. IOCTL Handler 0x22001B in the Amzetta zPortal DVM Tools <= v3.3.148.148 allow local attackers to execute arbitrary code in kernel mode or cause a denial of service (memory corruption and OS crash) via specially crafted I/O Request Packet.	8.8	More Details
CVE-2021-42979	NoMachine Cloud Server is affected by Integer Overflow. IOCTL Handler 0x22001B in the NoMachine Cloud Server above 4.0.346 and below 7.7.4 allow local attackers to execute arbitrary code in kernel mode or cause a denial of service (memory corruption and OS crash) via specially crafted I/O Request Packet.	8.8	More Details
CVE-2021-42977	NoMachine Enterprise Desktop is affected by Integer Overflow. IOCTL Handler 0x22001B in the NoMachine Enterprise Desktop above 4.0.346 and below 7.7.4 allow local attackers to execute arbitrary code in kernel mode or cause a denial of service (memory corruption and OS crash) via specially crafted I/O Request Packet.	8.8	More Details
CVE-2021-42976	NoMachine Enterprise Desktop is affected by Buffer Overflow. IOCTL Handler 0x22001B in the NoMachine Enterprise Desktop above 4.0.346 and below 7.7.4 allow local attackers to execute arbitrary code in kernel mode or cause a denial of service (memory corruption and OS crash) via specially crafted I/O Request Packet.	8.8	More Details
CVE-2021-43176	The GOautodial API prior to commit 3c3a979 made on October 13th, 2021 takes a user-supplied “action” parameter and appends a .php file extension to locate and load the correct PHP file to implement the API call. Vulnerable versions of GOautodial do not sanitize the user input that specifies the action. This permits an attacker to execute any PHP source file with a .php extension that is present on the disk and readable by the GOautodial web server process. Combined with CVE-2021-43175, it is possible for the attacker to do this without valid credentials. CVSS:3.1/AV:N/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H/E:P/RL:O/RC:C	8.8	More Details

CVE Number	Description	Base Score	Reference
CVE-2021-43040	An issue was discovered in Kaseya Unitrends Backup Appliance before 10.5.5. The privileged vaultServer could be leveraged to create arbitrary writable files, leading to privilege escalation.	8.8	More Details
CVE-2021-43041	An issue was discovered in Kaseya Unitrends Backup Appliance before 10.5.5. A crafted HTTP request could induce a format string vulnerability in the privileged vaultServer application.	8.8	More Details
CVE-2021-43415	HashiCorp Nomad and Nomad Enterprise up to 1.0.13, 1.1.7, and 1.2.0, with the QEMU task driver enabled, allowed authenticated users with job submission capabilities to bypass the configured allowed image paths. Fixed in 1.0.14, 1.1.8, and 1.2.1.	8.8	More Details
CVE-2021-43469	VINGA WR-N300U 77.102.1.4853 is affected by a command execution vulnerability in the goahead component.	8.8	More Details
CVE-2021-35413	A remote code execution (RCE) vulnerability in course_intro_pdf_import.php of Chamilo LMS v1.11.x allows authenticated attackers to execute arbitrary code via a crafted .htaccess file.	8.8	More Details
CVE-2021-29756	IBM Cognos Analytics 11.1.7 and 11.2.0 is vulnerable to cross-site request forgery (CSRF) in the My Inbox page which could allow an attacker to execute malicious and unauthorized actions transmitted from a user that the website trusts. IBM X-Force ID: 202167.	8.8	More Details
CVE-2020-12140	A buffer overflow in os/net/mac/ble/ble-l2cap.c in the BLE stack in Contiki-NG 4.4 and earlier allows an attacker to execute arbitrary code via malicious L2CAP frames.	8.8	More Details
CVE-2021-31631	b2evolution CMS v7.2.3 was discovered to contain a Cross-Site Request Forgery (CSRF) via the User login page. This vulnerability allows attackers to escalate privileges.	8.8	More Details
CVE-2020-36133	AOM v2.0.1 was discovered to contain a global buffer overflow via the component av1/encoder/partition_search.h.	8.8	More Details
CVE-2020-36131	AOM v2.0.1 was discovered to contain a stack buffer overflow via the component stats/rate_hist.c.	8.8	More Details
CVE-2020-36129	AOM v2.0.1 was discovered to contain a stack buffer overflow via the component src/aom_image.c.	8.8	More Details
CVE-2021-42972	NoMachine Server is affected by Buffer Overflow. IOCTL Handler 0x22001B in the NoMachine Server above 4.0.346 and below 7.7.4 allow local attackers to execute arbitrary code in kernel mode or cause a denial of service (memory corruption and OS crash) via specially crafted I/O Request Packet.	8.8	More Details

CVE Number	Description	Base Score	Reference
CVE-2021-42973	NoMachine Server is affected by Integer Overflow. IOCTL Handler 0x22001B in the NoMachine Server above 4.0.346 and below 7.7.4 allow local attackers to execute arbitrary code in kernel mode or cause a denial of service (memory corruption and OS crash) via specially crafted I/O Request Packet.	8.8	More Details
CVE-2021-40313	Piwigo v11.5 was discovered to contain a SQL injection vulnerability via the parameter pwg_token in /admin/batch_manager_global.php.	8.8	More Details
CVE-2021-43637	Amazon WorkSpaces agent is affected by Buffer Overflow. IOCTL Handler 0x22001B in the Amazon WorkSpaces agent below v1.0.1.1537 allow local attackers to execute arbitrary code in kernel mode or cause a denial of service (memory corruption and OS crash) via specially crafted I/O Request Packet.	8.8	More Details
CVE-2021-44227	In GNU Mailman before 2.1.38, a list member or moderator can get a CSRF token and craft an admin request (using that token) to set a new admin password or make other changes.	8.8	More Details
CVE-2021-42125	An unrestricted file upload vulnerability exists in Ivanti Avalanche before 6.3.3 allows an attacker with access to the Inforail Service to write dangerous files.	8.8	More Details
CVE-2021-42126	An improper authorization control vulnerability exists in Ivanti Avalanche before 6.3.3 allows an attacker with access to the Inforail Service to perform privilege escalation.	8.8	More Details
CVE-2021-42129	A command injection vulnerability exists in Ivanti Avalanche before 6.3.3 allows an attacker with access to the Inforail Service to perform arbitrary command execution.	8.8	More Details
CVE-2021-42687	A Buffer Overflow vulnerability exists in Accops HyWorks Windows Client prior to v 3.2.8.200. The IOCTL Handler 0x22005B allows local attackers to execute arbitrary code in kernel mode or cause a denial of service (memory corruption and OS crash) via specially crafted I/O Request Packet.	8.8	More Details
CVE-2021-4017	showdoc is vulnerable to Cross-Site Request Forgery (CSRF)	8.8	More Details
CVE-2021-20851	Cross-site request forgery (CSRF) vulnerability in Browser and Operating System Finder versions prior to 1.2 allows a remote unauthenticated attacker to hijack the authentication of an administrator via unspecified vectors.	8.8	More Details
CVE-2021-42685	An Integer Overflow vulnerability exists in Accops HyWorks DVM Tools prior to v3.3.1.105 . The IOCTL Handler 0x22005B in the Accops HyWorks DVM Tools prior to v3.3.1.105 allow local attackers to execute arbitrary code in kernel mode or cause a denial of service (memory corruption and OS crash) via specially crafted I/O Request Packet.	8.8	More Details

CVE Number	Description	Base Score	Reference
CVE-2021-42683	A Buffer Overflow vulnerability exists in Accops HyWorks Windows Client prior to v 3.2.8.200. The IOCTL Handler 0x22001B allows local attackers to execute arbitrary code in kernel mode or cause a denial of service (memory corruption and OS crash) via specially crafted I/O Request Packet.	8.8	More Details
CVE-2021-42682	An Integer Overflow vulnerability exists in Accops HyWorks DVM Tools prior to v3.3.1.105 .The IOCTL Handler 0x22001B allows local attackers to execute arbitrary code in kernel mode or cause a denial of service (memory corruption and OS crash) via specially crafted I/O Request Packet.	8.8	More Details
CVE-2021-43810	Admidio is a free open source user management system for websites of organizations and groups. A cross-site scripting vulnerability is present in Admidio prior to version 4.0.12. The Reflected XSS vulnerability occurs because redirect.php does not properly validate the value of the url parameter. Through this vulnerability, an attacker is capable to execute malicious scripts. This issue is patched in version 4.0.12.	8.8	More Details
CVE-2021-42688	An Integer Overflow vulnerability exists in Accops HyWorks Windows Client prior to v 3.2.8.200. The IOCTL Handler 0x22005B in the Accops HyWorks Windows Client prior to v 3.2.8.200 allow local attackers to execute arbitrary code in kernel mode or cause a denial of service (memory corruption and OS crash) via specially crafted I/O Request Packet.	8.8	More Details
CVE-2021-43360	Sunnet eHRD e-mail delivery task schedule’s serialization function has inadequate input object validation and restriction, which allows a post-authenticated remote attacker with database access privilege, to execute arbitrary code and control the system or interrupt services.	8.8	More Details
CVE-2021-42681	A Buffer Overflow vulnerability exists in Accops HyWorks DVM Tools prior to v3.3.1.105. The IOCTL Handler 0x22001B allows local attackers to execute arbitrary code in kernel mode or cause a denial of service (memory corruption and OS crash) via specially crafted I/O Request Packet.	8.8	More Details
CVE-2021-42124	An improper access control vulnerability exists in Ivanti Avalanche before 6.3.3 allows an attacker with access to the Inforail Service to perform a session takeover.	8.8	More Details
CVE-2021-43359	Sunnet eHRD has broken access control vulnerability, which allows a remote attacker to access account management page after being authenticated as a general user, then perform privilege escalation to execute arbitrary code and control the system or interrupt services.	8.8	More Details
CVE-2021-42130	A deserialization of untrusted data vulnerability exists in Ivanti Avalanche before 6.3.3 allows an attacker with access to the Inforail Service to perform arbitrary code execution.	8.8	More Details

CVE Number	Description	Base Score	Reference
CVE-2021-20864	Improper access control vulnerability in ELECOM routers (WRC-1167GST2 firmware v1.25 and prior, WRC-1167GST2A firmware v1.25 and prior, WRC-1167GST2H firmware v1.25 and prior, WRC-2533GS2-B firmware v1.52 and prior, WRC-2533GS2-W firmware v1.52 and prior, WRC-1750GS firmware v1.03 and prior, WRC-1750GSV firmware v2.11 and prior, WRC-1900GST firmware v1.03 and prior, WRC-2533GST firmware v1.03 and prior, WRC-2533GSTA firmware v1.03 and prior, WRC-2533GST2 firmware v1.25 and prior, WRC-2533GST2SP firmware v1.25 and prior, WRC-2533GST2-G firmware v1.25 and prior, and EDWRC-2533GST2 firmware v1.25 and prior) allows a network-adjacent unauthenticated attacker to bypass access restriction, and to start the telnet service and execute an arbitrary OS command via unspecified vectors.	8.8	More Details
CVE-2021-20861	Improper access control vulnerability in ELECOM LAN routers (WRC-1167GST2 firmware v1.25 and prior, WRC-1167GST2A firmware v1.25 and prior, WRC-1167GST2H firmware v1.25 and prior, WRC-2533GS2-B firmware v1.52 and prior, WRC-2533GS2-W firmware v1.52 and prior, WRC-1750GS firmware v1.03 and prior, WRC-1750GSV firmware v2.11 and prior, WRC-1900GST firmware v1.03 and prior, WRC-2533GST firmware v1.03 and prior, WRC-2533GSTA firmware v1.03 and prior, WRC-2533GST2 firmware v1.25 and prior, WRC-2533GST2SP firmware v1.25 and prior, WRC-2533GST2-G firmware v1.25 and prior, and EDWRC-2533GST2 firmware v1.25 and prior) allows a network-adjacent authenticated attacker to bypass access restriction and to access the management screen of the product via unspecified vectors.	8.8	More Details
CVE-2021-20860	Cross-site request forgery (CSRF) vulnerability in ELECOM LAN routers (WRC-1167GST2 firmware v1.25 and prior, WRC-1167GST2A firmware v1.25 and prior, WRC-1167GST2H firmware v1.25 and prior, WRC-2533GS2-B firmware v1.52 and prior, WRC-2533GS2-W firmware v1.52 and prior, WRC-1750GS firmware v1.03 and prior, WRC-1750GSV firmware v2.11 and prior, WRC-1900GST firmware v1.03 and prior, WRC-2533GST firmware v1.03 and prior, WRC-2533GSTA firmware v1.03 and prior, WRC-2533GST2 firmware v1.25 and prior, WRC-2533GST2SP firmware v1.25 and prior, WRC-2533GST2-G firmware v1.25 and prior, and EDWRC-2533GST2 firmware v1.25 and prior) allows a remote authenticated attacker to hijack the authentication of an administrator via a specially crafted page.	8.8	More Details
CVE-2021-42131	A SQL Injection vulnerability exists in Ivanti Avalance before 6.3.3 allows an attacker with access to the Inforail Service to perform privilege escalation.	8.8	More Details
CVE-2021-42132	A command Injection vulnerability exists in Ivanti Avalanche before 6.3.3 allows an attacker with access to the Inforail Service to perform arbitrary command execution.	8.8	More Details
CVE-2021-42686	An Integer Overflow exists in Accops HyWorks Windows Client prior to v 3.2.8.200. The IOCTL Handler 0x22001B in the Accops HyWorks Windows Client prior to v 3.2.8.200 allow local attackers to execute arbitrary code in kernel mode or cause a denial of service (memory corruption and OS crash) via specially crafted I/O Request Packet.	8.8	More Details

CVE Number	Description	Base Score	Reference
CVE-2021-37086	There is a Improper Preservation of Permissions vulnerability in Huawei Smartphone.Successful exploitation of this vulnerability may lead to attackers which can isolate and read synchronization files of other applications across the UID sandbox.	8.6	More Details
CVE-2021-40334	Missing Handler vulnerability in the proprietary management protocol (port TCP 5558) of Hitachi Energy FOX61x, XCM20 allows an attacker that exploits the vulnerability by activating SSH on port TCP 5558 to cause disruption to the NMS and NE communication. This issue affects: Hitachi Energy FOX61x versions prior to R15A. Hitachi Energy XCM20 versions prior to R15A.	8.6	More Details
CVE-2021-35245	When a user has admin rights in Serv-U Console, the user can move, create and delete any files are able to be accessed on the Serv-U host machine.	8.4	More Details
CVE-2021-36198	Successful exploitation of this vulnerability could allow an unauthorized user to access sensitive data.	8.3	More Details
CVE-2021-35242	Serv-U server responds with valid CSRFToken when the request contains only Session.	8.3	More Details
CVE-2021-23264	Installations, where crafter-search is not protected, allow unauthenticated remote attackers to create, view, and delete search indexes.	8.1	More Details
CVE-2021-42133	An exposed dangerous function vulnerability exists in Ivanti Avalanche before 6.3.3 allows an attacker with access to the Inforail Service to perform an arbitrary file write.	8.1	More Details
CVE-2021-23758	All versions of package ajaxpro.2 are vulnerable to Deserialization of Untrusted Data due to the possibility of deserialization of arbitrary .NET classes, which can be abused to gain remote code execution.	8.1	More Details
CVE-2021-43963	An issue was discovered in Couchbase Sync Gateway 2.7.0 through 2.8.2. The bucket credentials used to read and write data in Couchbase Server were insecurely being stored in the metadata within sync documents written to the bucket. Users with read access could use these credentials to obtain write access. (This issue does not affect clusters where Sync Gateway is authenticated with X.509 client certificates. This issue also does not affect clusters where shared bucket access is not enabled on Sync Gateway.)	8.1	More Details
CVE-2021-38575	NetworkPkg/IScsiDxe has remotely exploitable buffer overflows.	8.1	More Details

CVE Number	Description	Base Score	Reference
CVE-2021-28680	The devise_masquerade gem before 1.3 allows certain attacks when a password's salt is unknown. An application that uses this gem to let administrators masquerade/impersonate users loses one layer of security protection compared to a situation where Devise (without this extension) is used. If the server-side secret_key_base value became publicly known (for instance if it is committed to a public repository by mistake), there are still other protections in place that prevent an attacker from impersonating any user on the site. When masquerading is not used in a plain Devise application, one must know the password salt of the target user if one wants to encrypt and sign a valid session cookie. When devise_masquerade is used, however, an attacker can decide which user the "back" action will go back to without knowing that user's password salt and simply knowing the user ID, by manipulating the session cookie and pretending that a user is already masqueraded by an administrator.	8.1	More Details
CVE-2021-44480	Wokka Lokka Q50 devices through 2021-11-30 allow remote attackers (who know the SIM phone number and password) to listen to a device's surroundings via a callback in an SMS command, as demonstrated by the 123456 and 523681 default passwords.	8.1	More Details
CVE-2021-24914	The Tawk.To Live Chat WordPress plugin before 0.6.0 does not have capability and CSRF checks in the tawkto_setwidget and tawkto_removewidget AJAX actions, available to any authenticated user. The first one allows low-privileged users (including simple subscribers) to change the 'tawkto-embed-widget-page-id' and 'tawkto-embed-widget-widget-id' parameters. Any authenticated user can thus link the vulnerable website to their own Tawk.to instance. Consequently, they will be able to monitor the vulnerable website and interact with its visitors (receive contact messages, answer, ...). They will also be able to display an arbitrary Knowledge Base. The second one will remove the live chat widget from pages.	8.0	More Details
CVE-2021-20859	ELECOM LAN routers (WRC-1167GST2 firmware v1.25 and prior, WRC-1167GST2A firmware v1.25 and prior, WRC-1167GST2H firmware v1.25 and prior, WRC-2533GS2-B firmware v1.52 and prior, WRC-2533GS2-W firmware v1.52 and prior, WRC-1750GS firmware v1.03 and prior, WRC-1750GSV firmware v2.11 and prior, WRC-1900GST firmware v1.03 and prior, WRC-2533GST firmware v1.03 and prior, WRC-2533GSTA firmware v1.03 and prior, WRC-2533GST2 firmware v1.25 and prior, WRC-2533GST2SP firmware v1.25 and prior, WRC-2533GST2-G firmware v1.25 and prior, and EDWRC-2533GST2 firmware v1.25 and prior) allows a network-adjacent authenticated attacker to execute an arbitrary OS command via unspecified vectors.	8.0	More Details

CVE Number	Description	Base Score	Reference
CVE-2021-20863	OS command injection vulnerability in ELECOM routers (WRC-1167GST2 firmware v1.25 and prior, WRC-1167GST2A firmware v1.25 and prior, WRC-1167GST2H firmware v1.25 and prior, WRC-2533GS2-B firmware v1.52 and prior, WRC-2533GS2-W firmware v1.52 and prior, WRC-1750GS firmware v1.03 and prior, WRC-1750GSV firmware v2.11 and prior, WRC-1900GST firmware v1.03 and prior, WRC-2533GST firmware v1.03 and prior, WRC-2533GSTA firmware v1.03 and prior, WRC-2533GST2 firmware v1.25 and prior, WRC-2533GST2SP firmware v1.25 and prior, WRC-2533GST2-G firmware v1.25 and prior, and EDWRC-2533GST2 firmware v1.25 and prior) allows a network-adjacent authenticated attackers to execute an arbitrary OS command with the root privilege via unspecified vectors.	8.0	More Details
CVE-2021-44045	An out-of-bounds write vulnerability exists when reading a DGN file using Open Design Alliance Drawings SDK before 2022.11. The specific issue exists within the parsing of DGN files. Crafted data in a DGN file and lack of proper validation for the XFAT sectors count can trigger a write operation past the end of an allocated buffer. An attacker can leverage this vulnerability to execute code in the context of the current process.	7.8	More Details
CVE-2021-44046	An out-of-bounds write vulnerability exists when reading U3D files in Open Design Alliance PRC SDK before 2022.11. An unchecked return value of a function (verifying input data from a U3D file) leads to an out-of-bounds write. An attacker can leverage this vulnerability to execute code in the context of the current process.	7.8	More Details
CVE-2021-44019	An unnecessary privilege vulnerability in Trend Micro Worry-Free Business Security 10.0 SP1 could allow a local attacker to escalate privileges on affected installations. Please note: an attacker must first obtain the ability to execute low-privileged code on the target system in order to exploit this vulnerability. This vulnerability is similar to but not identical to CVE-2021-44020 and 44021.	7.8	More Details
CVE-2021-44047	A use-after-free vulnerability exists when reading a DWF/DWFX file using Open Design Alliance Drawings SDK before 2022.11. The specific issue exists with parsing DWF/DWFX files. Crafted data in a DWF/DWFX file and lack of proper validation of input data can trigger a write operation past the end of an allocated buffer. An attacker can leverage this vulnerability to execute code in the context of the current process.	7.8	More Details
CVE-2021-44044	An out-of-bounds write vulnerability exists when reading a JPG file using Open Design Alliance Drawings SDK before 2022.11. The specific issue exists with parsing JPG files. Crafted data in a JPG (4 extraneous bytes before the marker 0xca) can trigger a write operation past the end of an allocated buffer. An attacker can leverage this vulnerability to execute code in the context of the current process.	7.8	More Details

CVE Number	Description	Base Score	Reference
CVE-2021-44021	An unnecessary privilege vulnerability in Trend Micro Worry-Free Business Security 10.0 SP1 could allow a local attacker to escalate privileges on affected installations. Please note: an attacker must first obtain the ability to execute low-privileged code on the target system in order to exploit this vulnerability. This vulnerability is similar to but not identical to CVE-2021-44019 and 44020.	7.8	More Details
CVE-2021-44048	An out-of-bounds write vulnerability exists when reading a TIF file using Open Design Alliance (ODA) Drawings Explorer before 2022.11. The specific issue exists after loading TIF files. Crafted data in a TIF file can trigger a write operation past the end of an allocated buffer. An attacker can leverage this vulnerability to execute code in the context of the current process.	7.8	More Details
CVE-2020-29176	An arbitrary file upload vulnerability in Z-BlogPHP v1.6.1.2100 allows attackers to execute arbitrary code via a crafted JPG file.	7.8	More Details
CVE-2021-43034	An issue was discovered in Kaseya Unitrends Backup Appliance before 10.5.5. A world writable file allowed local users to execute arbitrary code as the user apache, leading to privilege escalation.	7.8	More Details
CVE-2021-4069	vim is vulnerable to Use After Free	7.8	More Details
CVE-2021-44020	An unnecessary privilege vulnerability in Trend Micro Worry-Free Business Security 10.0 SP1 could allow a local attacker to escalate privileges on affected installations. Please note: an attacker must first obtain the ability to execute low-privileged code on the target system in order to exploit this vulnerability. This vulnerability is similar to but not identical to CVE-2021-44019 and 44021.	7.8	More Details
CVE-2021-43037	An issue was discovered in Kaseya Unitrends Backup Appliance before 10.5.5. The Unitrends Windows agent was vulnerable to DLL injection and binary planting due to insecure default permissions. This allowed privilege escalation from an unprivileged user to SYSTEM.	7.8	More Details
CVE-2021-4019	vim is vulnerable to Heap-based Buffer Overflow	7.8	More Details
CVE-2021-42711	Barracuda Network Access Client before 5.2.2 creates a Temporary File in a Directory with Insecure Permissions. This file is executed with SYSTEM privileges when an unprivileged user performs a repair operation.	7.8	More Details
CVE-2021-32592	An unsafe search path vulnerability in FortiClientWindows 7.0.0, 6.4.6 and below, 6.2.x, 6.0.x and FortiClientEMS 7.0.0, 6.4.6 and below, 6.2.x, 6.0.x may allow an attacker to perform a DLL Hijack attack on affected devices via a malicious OpenSSL engine library in the search path.	7.8	More Details

CVE Number	Description	Base Score	Reference
CVE-2021-44149	An issue was discovered in Trusted Firmware OP-TEE Trusted OS through 3.15.0. The OPTEE-OS CSU driver for NXP i.MX6UL SoC devices lacks security access configuration for wakeup-related registers, resulting in TrustZone bypass because the NonSecure World can perform arbitrary memory read/write operations on Secure World memory. This involves a v cycle.	7.8	More Details
CVE-2021-3984	vim is vulnerable to Heap-based Buffer Overflow	7.8	More Details
CVE-2021-42776	CloverDX Server before 5.11.2 and and 5.12.x before 5.12.1 allows XXE during configuration import.	7.7	More Details
CVE-2021-37076	There is a Out-of-bounds Read vulnerability in Huawei Smartphone.Successful exploitation of this vulnerability may lead to availability affected.	7.5	More Details
CVE-2021-37068	There is a Resource Management Errors vulnerability in Huawei Smartphone.Successful exploitation of this vulnerability may lead to denial of Service Attacks.	7.5	More Details
CVE-2021-37046	There is a Memory leak vulnerability with the codec detection module in Huawei Smartphone.Successful exploitation of this vulnerability may cause the device to restart due to memory exhaustion.	7.5	More Details
CVE-2021-37067	There is a Exposure of Sensitive Information to an Unauthorized Actor vulnerability in Huawei Smartphone.Successful exploitation of this vulnerability may lead to Confidentiality impacted.	7.5	More Details
CVE-2021-22956	An uncontrolled resource consumption vulnerability exists in Citrix ADC <13.0-83.27, <12.1-63.22 and 11.1-65.23 that could allow an attacker with access to NSIP or SNIP with management interface access to cause a temporary disruption of the Management GUI, Nitro API, and RPC communication.	7.5	More Details
CVE-2021-37090	There is a Out-of-bounds Read vulnerability in Huawei Smartphone.Successful exploitation of this vulnerability may lead to process crash.	7.5	More Details
CVE-2021-37066	There is a Out-of-bounds Read vulnerability in Huawei Smartphone.Successful exploitation of this vulnerability may lead to process crash.	7.5	More Details
CVE-2021-22955	A unauthenticated denial of service vulnerability exists in Citrix ADC <13.0-83.27, <12.1-63.22 and 11.1-65.23 when configured as a VPN (Gateway) or AAA virtual server could allow an attacker to cause a temporary disruption of the Management GUI, Nitro API, and RPC communication.	7.5	More Details

CVE Number	Description	Base Score	Reference
CVE-2021-37061	There is a Uncontrolled Resource Consumption vulnerability in Huawei Smartphone.Successful exploitation of this vulnerability may lead to Screen projection application denial of service.	7.5	More Details
CVE-2021-37060	There is a Improper Input Validation vulnerability in Huawei Smartphone.Successful exploitation of this vulnerability may lead to SAMGR Heap Address Leakage.	7.5	More Details
CVE-2021-37057	There is a Improper Validation of Array Index vulnerability in Huawei Smartphone.Successful exploitation of this vulnerability may lead to restart the phone.	7.5	More Details
CVE-2021-37048	There is a Improper Input Validation vulnerability in Huawei Smartphone.Successful exploitation of this vulnerability may lead to fake visitors to control PC,play a video,etc.	7.5	More Details
CVE-2021-43471	In Canon LBP223 printers, the System Manager Mode login does not require an account password or PIN. An attacker can remotely shut down the device after entering the background, creating a denial of service vulnerability.	7.5	More Details
CVE-2021-37089	There is a Incomplete Cleanup vulnerability in Huawei Smartphone.Successful exploitation of this vulnerability may lead to kernel restart.	7.5	More Details
CVE-2021-37047	There is an Input verification vulnerability in Huawei Smartphone.Successful exploitation of this vulnerability may cause some services to restart.	7.5	More Details
CVE-2021-37072	There is a Incorrect Calculation of Buffer Size vulnerability in Huawei Smartphone.Successful exploitation of this vulnerability may lead to memory crash.	7.5	More Details
CVE-2021-43358	Sunnet eHRD has inadequate filtering for special characters in URLs, which allows a remote attacker to perform path traversal attacks without authentication, access restricted paths and download system files.	7.5	More Details
CVE-2021-37014	There is a Stack-based Buffer Overflow vulnerability in Huawei Smartphone.Successful exploitation of this vulnerability may lead to device cannot be used properly.	7.5	More Details
CVE-2021-37070	There is a Out-of-bounds Read vulnerability in Huawei Smartphone.Successful exploitation of this vulnerability may lead to process crash.	7.5	More Details
CVE-2021-24917	The WPS Hide Login WordPress plugin before 1.9.1 has a bug which allows to get the secret login page by setting a random referer string and making a request to /wp-admin/options.php as an unauthenticated user.	7.5	More Details

CVE Number	Description	Base Score	Reference
CVE-2021-37083	There is a NULL Pointer Dereference vulnerability in Huawei Smartphone.Successful exploitation of this vulnerability may lead to Denial of Service Attacks.	7.5	More Details
CVE-2021-37081	There is a Improper Input Validation vulnerability in Huawei Smartphone.Successful exploitation of this vulnerability may lead to nearby crash.	7.5	More Details
CVE-2021-44686	calibre before 5.32.0 contains a regular expression that is vulnerable to ReDoS (Regular Expression Denial of Service) in html_preprocess_rules in ebooks/conversion/preprocess.py.	7.5	More Details
CVE-2021-37071	There is a Business Logic Errors vulnerability in Huawei Smartphone.Successful exploitation of this vulnerability may lead to persistent dos.	7.5	More Details
CVE-2021-37080	There is a Incomplete Cleanup vulnerability in Huawei Smartphone.Successful exploitation of this vulnerability may lead to availability affected.	7.5	More Details
CVE-2021-37078	There is a Uncaught Exception vulnerability in Huawei Smartphone.Successful exploitation of this vulnerability may lead to remote Denial of Service.	7.5	More Details
CVE-2021-37077	There is a NULL Pointer Dereference vulnerability in Huawei Smartphone.Successful exploitation of this vulnerability may lead to kernel crash.	7.5	More Details
CVE-2021-43800	Wiki.js is a wiki app built on Node.js. Prior to version 2.5.254, directory traversal outside of Wiki.js context is possible when a storage module with local asset cache fetching is enabled on a Windows host. A malicious user can potentially read any file on the file system by crafting a special URL that allows for directory traversal. This is only possible on a Wiki.js server running on Windows, when a storage module implementing local asset cache (e.g Local File System or Git) is enabled and that no web application firewall solution (e.g. cloudflare) strips potentially malicious URLs. Commit number 414033de9dff66a327e3f3243234852f468a9d85 fixes this vulnerability by sanitizing the path before it is passed on to the storage module. The sanitization step removes any windows directory traversal sequences from the path. As a workaround, disable any storage module with local asset caching capabilities (Local File System, Git).	7.5	More Details
CVE-2021-37043	There is a Stack-based Buffer Overflow vulnerability in Huawei Smartphone.Successful exploitation of this vulnerability may lead to malicious application processes occupy system resources.	7.5	More Details

CVE Number	Description	Base Score	Reference
CVE-2021-40288	A denial-of-service attack in WPA2, and WPA3-SAE authentication methods in TP-Link AX10v1 before V1_211014, allows a remote unauthenticated attacker to disconnect an already connected wireless client via sending with a wireless adapter specific spoofed authentication frames	7.5	More Details
CVE-2021-42717	ModSecurity 3.x through 3.0.5 mishandles excessively nested JSON objects. Crafted JSON objects with nesting tens-of-thousands deep could result in the web server being unable to service legitimate requests. Even a moderately large (e.g., 300KB) HTTP request can occupy one of the limited NGINX worker processes for minutes and consume almost all of the available CPU on the machine. Modsecurity 2 is similarly vulnerable: the affected versions include 2.8.0 through 2.9.4.	7.5	More Details
CVE-2021-3980	elgg is vulnerable to Exposure of Private Personal Information to an Unauthorized Actor	7.5	More Details
CVE-2021-43795	Armeria is an open source microservice framework. In affected versions an attacker can access an Armeria server's local file system beyond its restricted directory by sending an HTTP request whose path contains `%2F` (encoded `/`), such as `/files/..%2Fsecrets.txt`, bypassing Armeria's path validation logic. Armeria 1.13.4 or above contains the hardened path validation logic that handles `%2F` properly. This vulnerability can be worked around by inserting a decorator that performs an additional validation on the request path.	7.5	More Details
CVE-2021-28236	LibreDWG v0.12.3 was discovered to contain a NULL pointer dereference via out_dxfb.c.	7.5	More Details
CVE-2021-37253	M-Files Web before 20.10.9524.1 allows a denial of service via overlapping ranges (in HTTP requests with crafted Range or Request-Range headers). NOTE: this is disputed because the range behavior is the responsibility of the web server, not the responsibility of the individual web application	7.5	More Details
CVE-2021-41039	In versions 1.6 to 2.0.11 of Eclipse Mosquitto, an MQTT v5 client connecting with a large number of user-property properties could cause excessive CPU usage, leading to a loss of performance and possible denial of service.	7.5	More Details
CVE-2021-37038	There is an Improper access control vulnerability in Huawei Smartphone.Successful exploitation of this vulnerability may affect service confidentiality.	7.5	More Details

CVE Number	Description	Base Score	Reference
CVE-2021-43798	Grafana is an open-source platform for monitoring and observability. Grafana versions 8.0.0-beta1 through 8.3.0 (except for patched versions) iss vulnerable to directory traversal, allowing access to local files. The vulnerable URL path is: `<grafana_host_url>/public/plugins//`, where is the plugin ID for any installed plugin. At no time has Grafana Cloud been vulnerable. Users are advised to upgrade to patched versions 8.0.7, 8.1.8, 8.2.7, or 8.3.1. The GitHub Security Advisory contains more information about vulnerable URL paths, mitigation, and the disclosure timeline.	7.5	More Details
CVE-2021-20400	IBM QRadar SIEM 7.3 and 7.4 uses weaker than expected cryptographic algorithms that could allow an attacker to decrypt highly sensitive information. IBM X-Force ID: 196074.	7.5	More Details
CVE-2021-43805	Solidus is a free, open-source ecommerce platform built on Rails. Versions of Solidus prior to 3.1.4, 3.0.4, and 2.11.13 have a denial of service vulnerability that could be exploited during a guest checkout. The regular expression used to validate a guest order's email was subject to exponential backtracking through a fragment like `a.a.` Versions 3.1.4, 3.0.4, and 2.11.13 have been patched to use a different regular expression. The maintainers added a check for email addresses that are no longer valid that will print information about any affected orders that exist. If a prompt upgrade is not an option, a workaround is available. It is possible to edit the file `config/application.rb` manually (with code provided by the maintainers in the GitHub Security Advisory) to check email validity.	7.5	More Details
CVE-2021-20611	Improper Input Validation vulnerability in Mitsubishi Electric MELSEC iQ-R Series R00/01/02CPU, MELSEC iQ-R Series R04/08/16/32/120(EN)CPU, MELSEC iQ-R Series R08/16/32/120SFCPU, MELSEC iQ-R Series R08/16/32/120PCPU, MELSEC iQ-R Series R08/16/32/120PSFCPU, MELSEC iQ-R Series R16/32/64MTCPU, MELSEC iQ-R Series R12CCPU-V, MELSEC Q Series Q03UDECPU, MELSEC Q Series Q04/06/10/13/20/26/50/100UDEHCPU, MELSEC Q Series Q03/04/06/13/26UDVCPU, MELSEC Q Series Q04/06/13/26UDPVCPU, MELSEC Q Series Q12DCCPU-V, MELSEC Q Series Q24DHCCPU-V(G), MELSEC Q Series Q24/26DHCCPU-LS, MELSEC Q Series MR-MQ100, MELSEC Q Series Q172/173DCPU-S1, MELSEC Q Series Q172/173DSCPU, MELSEC Q Series Q170MCPU, MELSEC Q Series Q170MSCPU(-S1), MELSEC L Series L02/06/26CPU(-P), MELSEC L Series L26CPU-(P)BT and MELIPC Series MI5122-VW allows a remote unauthenticated attacker to cause a denial-of-service (DoS) condition by sending specially crafted packets. System reset is required for recovery.	7.5	More Details
CVE-2021-20470	IBM Cognos Analytics 11.1.7 and 11.2.0 does not require that users should have strong passwords by default, which makes it easier for attackers to compromise user accounts. IBM X-Force ID: 196339.	7.5	More Details

CVE Number	Description	Base Score	Reference
CVE-2021-20610	Improper Handling of Length Parameter Inconsistency vulnerability in Mitsubishi Electric MELSEC iQ-R Series R00/01/02CPU, MELSEC iQ-R Series R04/08/16/32/120(EN)CPU, MELSEC iQ-R Series R08/16/32/120SFCPU, MELSEC iQ-R Series R08/16/32/120PCPU, MELSEC iQ-R Series R08/16/32/120PSFCPU, MELSEC iQ-R Series R16/32/64MTCPU, MELSEC iQ-R Series R12CCPU-V, MELSEC Q Series Q03UDECPU, MELSEC Q Series Q04/06/10/13/20/26/50/100UDEHCPU, MELSEC Q Series Q03/04/06/13/26UDVCPU, MELSEC Q Series Q04/06/13/26UDPVCPU, MELSEC Q Series Q12DCCPU-V, MELSEC Q Series Q24DHCCPU-V(G), MELSEC Q Series Q24/26DHCCPU-LS, MELSEC Q Series MR-MQ100, MELSEC Q Series Q172/173DCPU-S1, MELSEC Q Series Q172/173DSCPU, MELSEC Q Series Q170MCPU, MELSEC Q Series Q170MSCPU(-S1), MELSEC L Series L02/06/26CPU(-P), MELSEC L Series L26CPU-(P)BT and MELIPC Series MI5122-VW allows a remote unauthenticated attacker to cause a denial-of-service (DoS) condition by sending specially crafted packets. System reset is required for recovery.	7.5	More Details
CVE-2021-43175	The GOautodial API prior to commit 3c3a979 made on October 13th, 2021 exposes an API router that accepts a username, password, and action that routes to other PHP files that implement the various API functions. Vulnerable versions of GOautodial validate the username and password incorrectly, allowing the caller to specify any values for these parameters and successfully authenticate. CVSS:3.1/AV:N/AC:L/PR:N/UI:N/S:U/C:L/I:N/A:N/E:P/RL:O/RC:C	7.5	More Details
CVE-2021-43789	PrestaShop is an Open Source e-commerce web application. Versions of PrestaShop prior to 1.7.8.2 are vulnerable to blind SQL injection using search filters with `orderBy` and `sortOrder` parameters. The problem is fixed in version 1.7.8.2.	7.5	More Details
CVE-2021-37100	There is a Improper Authentication vulnerability in Huawei Smartphone.Successful exploitation of this vulnerability may lead to account authentication bypassed.	7.5	More Details
CVE-2021-37096	There is a Improper Input Validation vulnerability in Huawei Smartphone.Successful exploitation of this vulnerability may lead to user privacy disclosed.	7.5	More Details
CVE-2021-37094	There is a Improper Input Validation vulnerability in Huawei Smartphone.Successful exploitation of this vulnerability may lead to system denial of service.	7.5	More Details

CVE Number	Description	Base Score	Reference
CVE-2021-20609	Uncontrolled Resource Consumption vulnerability in Mitsubishi Electric MELSEC iQ-R Series R00/01/02CPU, MELSEC iQ-R Series R04/08/16/32/120(EN)CPU, MELSEC iQ-R Series R08/16/32/120SFCPU, MELSEC iQ-R Series R08/16/32/120PCPU, MELSEC iQ-R Series R08/16/32/120PSFCPU, MELSEC iQ-R Series R16/32/64MTCPU, MELSEC iQ-R Series R12CCPU-V, MELSEC Q Series Q03UDECPU, MELSEC Q Series Q04/06/10/13/20/26/50/100UDEHCPU, MELSEC Q Series Q03/04/06/13/26UDVCPU, MELSEC Q Series Q04/06/13/26UDPVCPU, MELSEC Q Series Q12DCCPU-V, MELSEC Q Series Q24DHCCPU-V(G), MELSEC Q Series Q24/26DHCCPU-LS, MELSEC Q Series MR-MQ100, MELSEC Q Series Q172/173DCPU-S1, MELSEC Q Series Q172/173DSCPU, MELSEC Q Series Q170MCPU, MELSEC Q Series Q170MSCPU(-S1), MELSEC L Series L02/06/26CPU(-P), MELSEC L Series L26CPU-(P)BT and MELIPC Series MI5122-VW allows a remote unauthenticated attacker to cause a denial-of-service (DoS) condition by sending specially crafted packets. System reset is required for recovery.	7.5	More Details
CVE-2021-37091	There is a Permissions,Privileges,and Access Controls vulnerability in Huawei Smartphone.Successful exploitation of this vulnerability may lead to confidentiality affected.	7.5	More Details
CVE-2021-34543	The web administration server in Solar-Log 500 before 2.8.2 Build 52 does not require authentication, which allows remote attackers to gain administrative privileges by connecting to the server. As a result, the attacker can modify configuration files and change the system status. Fixed with 3.0.0-60 11.10.2013 for SL 200, 500, 1000 / not existing for SL 250, 300, 1200, 2000, SL 50 Gateway, SL Base.	7.5	More Details
CVE-2021-34599	Affected versions of CODESYS Git in Versions prior to V1.1.0.0 lack certificate validation in HTTPS handshakes. CODESYS Git does not implement certificate validation by default, so it does not verify that the server provides a valid and trusted HTTPS certificate. Since the certificate of the server to which the connection is made is not properly verified, the server connection is vulnerable to a man-in-the-middle attack.	7.4	More Details
CVE-2020-10627	Insulet Omnipod Insulin Management System insulin pump product ID 19191 and 40160 is designed to communicate using a wireless RF with an Insulet manufactured Personal Diabetes Manager device. This wireless RF communication protocol does not properly implement authentication or authorization. An attacker with access to one of the affected insulin pump models may be able to modify and/or intercept data. This vulnerability could also allow attackers to change pump settings and control insulin delivery.	7.3	More Details
CVE-2021-40578	Authenticated Blind & Error-based SQL injection vulnerability was discovered in Online Enrollment Management System in PHP and PayPal Free Source Code 1.0, that allows attackers to obtain sensitive information and execute arbitrary SQL commands via IDNO parameter.	7.2	More Details

CVE Number	Description	Base Score	Reference
CVE-2021-4075	snipe-it is vulnerable to Server-Side Request Forgery (SSRF)	7.2	More Details
CVE-2021-25784	Taocms v2.5Beta5 was discovered to contain a blind SQL injection vulnerability via the function Edit Article.	7.2	More Details
CVE-2020-35012	The Events Manager WordPress plugin before 5.9.8 does not sanitise and escape a parameter before using it in a SQL statement, leading to an SQL Injection	7.2	More Details
CVE-2021-25783	Taocms v2.5Beta5 was discovered to contain a blind SQL injection vulnerability via the function Article Search.	7.2	More Details
CVE-2021-36133	The OPTEE-OS CSU driver for NXP i.MX SoC devices lacks security access configuration for several models, resulting in TrustZone bypass because the NonSecure World can perform arbitrary memory read/write operations on Secure World memory. This involves a DMA capable peripheral.	7.1	More Details
CVE-2021-44512	World-writable permissions on the /tmp/tmate/sessions directory in tmate-ssh-server 2.3.0 allow a local attacker to compromise the integrity of session handling, or obtain the read-write session ID from a read-only session symlink in this directory.	7.0	More Details
CVE-2021-44513	Insecure creation of temporary directories in tmate-ssh-server 2.3.0 allows a local attacker to compromise the integrity of session handling.	7.0	More Details
CVE-2021-28703	grant table v2 status pages may remain accessible after de-allocation (take two) Guest get permitted access to certain Xen-owned pages of memory. The majority of such pages remain allocated / associated with a guest for its entire lifetime. Grant table v2 status pages, however, get de-allocated when a guest switched (back) from v2 to v1. The freeing of such pages requires that the hypervisor know where in the guest these pages were mapped. The hypervisor tracks only one use within guest space, but racing requests from the guest to insert mappings of these pages may result in any of them to become mapped in multiple locations. Upon switching back from v2 to v1, the guest would then retain access to a page that was freed and perhaps re-used for other purposes. This bug was fortuitously fixed by code cleanup in Xen 4.14, and backported to security-supported Xen branches as a prerequisite of the fix for XSA-378.	7.0	More Details

CVE Number	Description	Base Score	Reference
CVE-2021-44518	An issue was discovered in the eGeeTouch 3rd Generation Travel Padlock application for Android. The lock sends a pairing code before each operation (lock or unlock) activated via the companion app. The code is sent unencrypted, allowing any attacker with the same app (either Android or iOS) to add the lock and take complete control. For successful exploitation, the attacker must be able to touch the lock's power button, and must be able to capture BLE network communication.	6.8	More Details
CVE-2021-20854	ELECOM LAN routers (WRH-733GBK firmware v1.02.9 and prior and WRH-733GWH firmware v1.02.9 and prior) allows a network-adjacent attacker with an administrator privilege to execute arbitrary OS commands via unspecified vectors.	6.8	More Details
CVE-2021-37940	An information disclosure via GET request server-side request forgery vulnerability was discovered with the Workplace Search Github Enterprise Server integration. Using this vulnerability, a malicious Workplace Search admin could use the GHES integration to view hosts that might not be publicly accessible.	6.8	More Details
CVE-2021-43991	The Kentico Xperience CMS version 13.0 – 13.0.43 is vulnerable to a persistent Cross-Site Scripting (XSS) vulnerability (also known as Stored or Second-Order XSS). Persistent XSS vulnerabilities occur when the application stores and retrieves client supplied data without proper handling of dangerous content. This type of XSS vulnerability is exploited by submitting malicious script content to the application which is then retrieved and executed by other application users. The attacker could exploit this to conduct a range of attacks against users of the affected application such as session hijacking, account take over and accessing sensitive data.	6.8	More Details
CVE-2021-20853	ELECOM LAN routers (WRH-733GBK firmware v1.02.9 and prior and WRH-733GWH firmware v1.02.9 and prior) allows a network-adjacent attacker with an administrator privilege to execute arbitrary OS commands via unspecified vectors.	6.8	More Details
CVE-2021-20852	Buffer overflow vulnerability in ELECOM LAN routers (WRH-733GBK firmware v1.02.9 and prior and WRH-733GWH firmware v1.02.9 and prior) allows a network-adjacent attacker with an administrator privilege to execute an arbitrary OS command via unspecified vectors.	6.8	More Details
CVE-2021-3944	bookstack is vulnerable to Cross-Site Request Forgery (CSRF)	6.8	More Details
CVE-2021-3993	showdoc is vulnerable to Cross-Site Request Forgery (CSRF)	6.5	More Details

CVE Number	Description	Base Score	Reference
CVE-2021-3990	showdoc is vulnerable to Use of Cryptographically Weak Pseudo-Random Number Generator (PRNG)	6.5	More Details
CVE-2021-3992	kimai2 is vulnerable to Improper Access Control	6.5	More Details
CVE-2021-34544	An issue was discovered in Solar-Log 500 before 2.8.2 Build 52 23.04.2013. In /export.html, email.html, and sms.html, cleartext passwords are stored. This may allow sensitive information to be read by someone with access to the device. Fixed with 3.0.0-60 11.10.2013 for SL 200, 500, 1000 / not existing for SL 250, 300, 1200, 2000, SL 50 Gateway, SL Base.	6.5	More Details
CVE-2021-43039	An issue was discovered in Kaseya Unitrends Backup Appliance before 10.5.5. The Samba file sharing service allowed anonymous read/write access.	6.5	More Details
CVE-2021-4049	livehelperchat is vulnerable to Cross-Site Request Forgery (CSRF)	6.5	More Details
CVE-2021-43791	Zulip is an open source group chat application that combines real-time chat with threaded conversations. In affected versions expiration dates on the confirmation objects associated with email invitations were not enforced properly in the new account registration flow. A confirmation link takes a user to the check_prereg_key_and_redirect endpoint, before getting redirected to POST to /accounts/register/. The problem was that validation was happening in the check_prereg_key_and_redirect part and not in /accounts/register/ - meaning that one could submit an expired confirmation key and be able to register. The issue is fixed in Zulip 4.8. There are no known workarounds and users are advised to upgrade as soon as possible.	6.5	More Details
CVE-2021-23260	Authenticated users with Site roles may inject XSS scripts via file names that will execute in the browser for this and other users of the same site.	6.5	More Details
CVE-2021-44050	CA Network Flow Analysis (NFA) 21.2.1 and earlier contain a SQL injection vulnerability in the NFA web application, due to insufficient input validation, that could potentially allow an authenticated user to access sensitive data.	6.5	More Details
CVE-2020-36130	AOM v2.0.1 was discovered to contain a NULL pointer dereference via the component av1/av1_dx_iface.c.	6.5	More Details
CVE-2020-36134	AOM v2.0.1 was discovered to contain a segmentation violation via the component aom_dsp/x86/obmc_sad_avx2.c.	6.5	More Details

CVE Number	Description	Base Score	Reference
CVE-2020-36135	AOM v2.0.1 was discovered to contain a NULL pointer dereference via the component rate_hist.c.	6.5	More Details
CVE-2021-29716	IBM Cognos Analytics 11.1.7 and 11.2.0 could allow a low level user to reas of the application that privileged user should only be allowed to view. IBM X-Force ID: 201087.	6.5	More Details
CVE-2021-43043	An issue was discovered in Kaseya Unitrends Backup Appliance before 10.5.5. The apache user could read arbitrary files such as /etc/shadow by abusing an insecure Sudo rule.	6.5	More Details
CVE-2021-44527	A vulnerability found in UniFi Switch firmware Version 5.43.35 and earlier allows a malicious actor who has already gained access to the network to perform a Deny of Service (DoS) attack on the affected switch.This vulnerability is fixed in UniFi Switch firmware 5.76.6 and later.	6.5	More Details
CVE-2021-43781	Invenio-Drafts-Resources is a submission/deposit module for Invenio, a software framework for research data management. Invenio-Drafts-Resources prior to versions 0.13.7 and 0.14.6 does not properly check permissions when a record is published. The vulnerability is exploitable in a default installation of InvenioRDM. An authenticated a user is able via REST API calls to publish draft records of other users if they know the record identifier and the draft validates (e.g. all require fields filled out). An attacker is not able to modify the data in the record, and thus e.g. *cannot* change a record from restricted to public. The problem is patched in Invenio-Drafts-Resources v0.13.7 and 0.14.6, which is part of InvenioRDM v6.0.1 and InvenioRDM v7.0 respectively.	6.4	More Details
CVE-2021-22170	Assuming a database breach, nonce reuse issues in GitLab 11.6+ allows an attacker to decrypt some of the database's encrypted content	6.2	More Details
CVE-2021-36760	In accountrecoveryendpoint/recoverpassword.do in WSO2 Identity Server 5.7.0, it is possible to perform a DOM-Based XSS attack affecting the callback parameter modifying the URL that precedes the callback parameter. Once the username or password reset procedure is completed, the JavaScript code will be executed. (recoverpassword.do also has an open redirect issue for a similar reason.)	6.1	More Details
CVE-2021-42567	Apereo CAS through 6.4.1 allows XSS via POST requests sent to the REST API endpoints.	6.1	More Details
CVE-2021-44148	GL.iNet GL-AR150 2.x before 3.x devices, configured as repeaters, allow cgi-bin/router_cgi?action=scanwifi XSS when an attacker creates an SSID with an XSS payload as the name.	6.1	More Details

CVE Number	Description	Base Score	Reference
CVE-2020-19611	Cross Site Scripting (XSS) in redirect module of Racktables version 0.21.2, allows an attacker to inject arbitrary web script or HTML via the op parameter.	6.1	More Details
CVE-2021-43689	manage (last update Oct 24, 2017) is affected by a Cross Site Scripting (XSS) vulnerability in Application/Home/Controller/GoodsController.class.php. The exit function will terminate the script and print a message which have values from $_POST.	6.1	More Details
CVE-2021-4000	showdoc is vulnerable to URL Redirection to Untrusted Site	6.1	More Details
CVE-2021-43673	dzzoffice 2.02.1_SC_UTF8 is affected by a Cross Site Scripting (XSS) vulnerability in explorerfile.php. The output of the exit function is printed for the user via exit(json_encode($return)).	6.1	More Details
CVE-2021-20493	IBM Cognos Analytics 11.1.7 and 11.2.0 is vulnerable to cross-site scripting. This vulnerability allows users to embed arbitrary JavaScript code in the Web UI thus altering the intended functionality potentially leading to credentials disclosure within a trusted session. IBM X-Force ID: 197794.	6.1	More Details
CVE-2021-43686	nZEDb v0.4.20 is affected by a Cross Site Scripting (XSS) vulnerability in www/pages/api.php. The exit function will terminate the script and print the message which has the input $_GET['t'].	6.1	More Details
CVE-2021-43683	pictshare v1.5 is affected by a Cross Site Scripting (XSS) vulnerability in api/info.php. The exit function will terminate the script and print the message which has $_REQUEST['hash'].	6.1	More Details
CVE-2021-43681	SakuraPanel v1.0.1.1 is affected by a Cross Site Scripting (XSS) vulnerability in /master/core/PostHandler.php. The exit function will terminate the script and print the message $data['proxy_name'].	6.1	More Details
CVE-2020-35037	The Events Manager WordPress plugin before 5.9.8 does not sanitise and escape some search parameter before outputing them in pages, which could lead to Cross-Site Scripting issues	6.1	More Details
CVE-2021-29849	IBM QRadar SIEM 7.3 and 7.4 is vulnerable to cross-site scripting. This vulnerability allows users to embed arbitrary JavaScript code in the Web UI thus altering the intended functionality potentially leading to credentials disclosure within a trusted session. IBM X-Force ID: 205281.	6.1	More Details
CVE-2021-43687	chamilo-lms v1.11.14 is affected by a Cross Site Scripting (XSS) vulnerability in /plugin/jcapture/applet.php if an attacker passes a message hex2bin in the cookie.	6.1	More Details
CVE-2021-24924	The Email Log WordPress plugin before 2.4.8 does not escape the d parameter before outputting it back in an attribute in the Log page, leading to a Reflected Cross-Site Scripting issue	6.1	More Details

CVE Number	Description	Base Score	Reference
CVE-2021-24935	The WP Google Fonts WordPress plugin before 3.1.5 does not escape the googlefont_ajax_name and googlefont_ajax_family parameter of the googlefont_action AJAx action (available to any authenticated user) before outputing them in attributes, leading Reflected Cross-Site Scripting issues	6.1	More Details
CVE-2021-24938	The WOOCS WordPress plugin before 1.3.7.1 does not sanitise and escape the key parameter of the woocs_update_profiles_data AJAX action (available to any authenticated user) before outputting it back in the response, leading to a Reflected cross-Site Scripting issue	6.1	More Details
CVE-2021-25041	The Photo Gallery by 10Web WordPress plugin before 1.5.68 is vulnerable to Reflected Cross-Site Scripting (XSS) issues via the bwg_album_breadcrumb_0 and shortcode_id GET parameters passed to the bwg_frontend_data AJAX action	6.1	More Details
CVE-2021-44479	NXP Kinetis K82 devices have a buffer over-read via a crafted wlength value in a GET Status-Other request during use of USB In-System Programming (ISP) mode. This discloses protected flash memory.	6.1	More Details
CVE-2021-24939	The LoginWP (Formerly Peter's Login Redirect) WordPress plugin before 3.0.0.5 does not sanitise and escape the rul_login_url and rul_logout_url parameter before outputting them back in attributes in an admin page, leading to a Reflected Cross-Site Scripting issue	6.1	More Details
CVE-2021-43682	thinkphp-bjyblog (last update Jun 4 2021) is affected by a Cross Site Scripting (XSS) vulnerability in AdminBaseController.class.php. The exit function terminates the script and prints a message to the user that contains $_SERVER['HTTP_HOST'].	6.1	More Details
CVE-2021-43690	YurunProxy v0.01 is affected by a Cross Site Scripting (XSS) vulnerability in src/Client.php. The exit function will terminate the script and print a message which have values from the socket_read.	6.1	More Details
CVE-2021-44279	Librenms 21.11.0 is affected by a Cross Site Scripting (XSS) vulnerability in includes/html/forms/poller-groups.inc.php.	6.1	More Details
CVE-2021-44277	Librenms 21.11.0 is affected by a Cross Site Scripting (XSS) vulnerability in includes/html/common/alert-log.inc.php.	6.1	More Details
CVE-2021-20847	Cross-site scripting vulnerability in Wi-Fi STATION SH-52A (38JP_1_11G, 38JP_1_11J, 38JP_1_11K, 38JP_1_11L, 38JP_1_26F, 38JP_1_26G, 38JP_1_26J, 38JP_2_03B, and 38JP_2_03C) allows a remote unauthenticated attacker to inject an arbitrary script via WebUI of the device.	6.1	More Details

CVE Number	Description	Base Score	Reference
CVE-2021-29116	A stored Cross Site Scripting (XSS) vulnerability in Esri ArcGIS Server feature services versions 10.8.1 and 10.9 (only) feature services may allow a remote, unauthenticated attacker to pass and store malicious strings via crafted queries which when accessed could potentially execute arbitrary JavaScript code in the user's browser.	6.1	More Details
CVE-2021-3989	showdoc is vulnerable to URL Redirection to Untrusted Site	6.1	More Details
CVE-2021-40154	NXP LPC55S69 devices before A3 have a buffer over-read via a crafted wlength value in a GET Descriptor Configuration request during use of USB In-System Programming (ISP) mode. This discloses protected flash memory.	6.1	More Details
CVE-2021-3983	kimai2 is vulnerable to Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	6.1	More Details
CVE-2021-43784	runc is a CLI tool for spawning and running containers on Linux according to the OCI specification. In runc, netlink is used internally as a serialization system for specifying the relevant container configuration to the `C` portion of the code (responsible for the based namespace setup of containers). In all versions of runc prior to 1.0.3, the encoder did not handle the possibility of an integer overflow in the 16-bit length field for the byte array attribute type, meaning that a large enough malicious byte array attribute could result in the length overflowing and the attribute contents being parsed as netlink messages for container configuration. This vulnerability requires the attacker to have some control over the configuration of the container and would allow the attacker to bypass the namespace restrictions of the container by simply adding their own netlink payload which disables all namespaces. The main users impacted are those who allow untrusted images with untrusted configurations to run on their machines (such as with shared cloud infrastructure). runc version 1.0.3 contains a fix for this bug. As a workaround, one may try disallowing untrusted namespace paths from your container. It should be noted that untrusted namespace paths would allow the attacker to disable namespace protections entirely even in the absence of this bug.	6.0	More Details
CVE-2021-37085	There is a Encoding timing vulnerability in Huawei Smartphone.Successful exploitation of this vulnerability may lead to denial of service.	5.9	More Details
CVE-2021-37082	There is a Race Condition vulnerability in Huawei Smartphone.Successful exploitation of this vulnerability may lead to motionhub crash.	5.9	More Details
CVE-2021-3964	elgg is vulnerable to Authorization Bypass Through User-Controlled Key	5.9	More Details

CVE Number	Description	Base Score	Reference
CVE-2020-27414	Mahavitaran android application 7.50 and prior transmit sensitive information in URL parameters. This may lead to information disclosure if unauthorized parties have access to the URLs via server logs, referrer header, MITM or browser history.	5.9	More Details
CVE-2021-23263	Unauthenticated remote attackers can read textual content via FreeMarker including files /scripts/*, /templates/* and some of the files in /.git/* (non-binary).	5.9	More Details
CVE-2021-29779	IBM QRadar SIEM 7.3 and 7.4 could allow an attacker to obtain sensitive information due to the server performing key exchange without entity authentication on inter-host communications using man in the middle techniques. IBM X-Force ID: 203033.	5.9	More Details
CVE-2021-44022	A reachable assertion vulnerability in Trend Micro Apex One could allow an attacker to crash the program on affected installations, leading to a denial-of-service (DoS). Please note: an attacker must first obtain the ability to execute low-privileged code on the target system in order to exploit this vulnerability.	5.5	More Details
CVE-2021-43772	Trend Micro Security 2021 v17.0 (Consumer) contains a vulnerability that allows files inside the protected folder to be modified without any detection.	5.5	More Details
CVE-2020-27356	The debug-meta-data plugin 1.1.2 for WordPress allows XSS.	5.4	More Details
CVE-2021-25967	In CKAN, versions 2.9.0 to 2.9.3 are affected by a stored XSS vulnerability via SVG file upload of users' profile picture. This allows low privileged application users to store malicious scripts in their profile picture. These scripts are executed in a victim's browser when they open the malicious profile picture	5.4	More Details
CVE-2021-4018	snipe-it is vulnerable to Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting')	5.4	More Details
CVE-2021-20858	Cross-site scripting vulnerability in ELECOM LAN router WRC-2533GHBK-I firmware v1.20 and prior allows a remote authenticated attacker to inject an arbitrary script via unspecified vectors.	5.4	More Details
CVE-2021-20857	Cross-site scripting vulnerability in ELECOM LAN router WRC-2533GHBK-I firmware v1.20 and prior allows a remote authenticated attacker to inject an arbitrary script via unspecified vectors.	5.4	More Details
CVE-2021-20856	Cross-site scripting vulnerability in ELECOM LAN routers (WRH-733GBK firmware v1.02.9 and prior and WRH-733GWH firmware v1.02.9 and prior) allows a remote authenticated attacker to inject an arbitrary script via unspecified vectors.	5.4	More Details

CVE Number	Description	Base Score	Reference
CVE-2021-20855	Cross-site scripting vulnerability in ELECOM LAN routers (WRH-733GBK firmware v1.02.9 and prior and WRH-733GWH firmware v1.02.9 and prior) allows a remote authenticated attacker to inject an arbitrary script via unspecified vectors.	5.4	More Details
CVE-2021-24759	The PDF.js Viewer WordPress plugin before 2.0.2 does not escape some of its shortcode and Gutenberg Block attributes, which could allow users with a role as low as Contributor to to perform Cross-Site Scripting attacks	5.4	More Details
CVE-2021-24930	The WordPress Online Booking and Scheduling Plugin WordPress plugin before 20.3.1 does not escape the Staff Full Name field before outputting it back in a page, which could lead to a Stored Cross-Site Scripting issue	5.4	More Details
CVE-2021-40096	A cross-site scripting (XSS) vulnerability in integration configuration in SquaredUp for SCOM 5.2.1.6654 allows remote attackers to inject arbitrary web script or HTML via modification of the authorisationUrl in some integration configurations.	5.4	More Details
CVE-2021-29867	IBM Cognos Analytics 11.1.7 and 11.2.0 could allow an authenticated to view or edit a Jupyter notebook that they should not have access to. IBM X-Force ID: 206212.	5.4	More Details
CVE-2021-38909	IBM Cognos Analytics 11.1.7 and 11.2.0 is vulnerable to cross-site scripting. This vulnerability allows users to embed arbitrary JavaScript code in the Web UI thus altering the intended functionality potentially leading to credentials disclosure within a trusted session. IBM X-Force ID: 209706.	5.4	More Details
CVE-2021-40094	A DOM-based XSS vulnerability affects SquaredUp for SCOM 5.2.1.6654. If successfully exploited, this vulnerability may allow attackers to inject malicious code into a user's device.	5.4	More Details
CVE-2021-40093	A cross-site scripting (XSS) vulnerability in integration configuration in SquaredUp for SCOM 5.2.1.6654 allows remote attackers to inject arbitrary web script or HTML via dashboard actions.	5.4	More Details
CVE-2021-40092	A cross-site scripting (XSS) vulnerability in Image Tile in SquaredUp for SCOM 5.2.1.6654 allows remote attackers to inject arbitrary web script or HTML via an SVG file.	5.4	More Details
CVE-2021-37055	There is a Logic bypass vulnerability in Huawei Smartphone.Successful exploitation of this vulnerability may allow attempts to obtain certain device information.	5.3	More Details
CVE-2021-37056	There is an Improper permission control vulnerability in Huawei Smartphone.Successful exploitation of this vulnerability may allow attempts to obtain certain device information.	5.3	More Details
CVE-2021-37058	There is a Permissions,Privileges,and Access Controls vulnerability in Huawei Smartphone.Successful exploitation of this vulnerability may lead to the user's nickname is maliciously tampered with.	5.3	More Details

CVE Number	Description	Base Score	Reference
CVE-2021-29719	IBM Cognos Analytics 11.1.7 and 11.2.0 could be vulnerable to client side vulnerabilties due to a web response specifying an incorrect content type. IBM X-Force ID: 201091	5.3	More Details
CVE-2021-43794	Discourse is an open source discussion platform. In affected versions an attacker can poison the cache for anonymous (i.e. not logged in) users, such that the users are shown a JSON blob instead of the HTML page. This can lead to a partial denial-of-service. This issue is patched in the latest stable, beta and tests-passed versions of Discourse.	5.3	More Details
CVE-2021-29115	An information disclosure vulnerability in the ArcGIS Service Directory in Esri ArcGIS Enterprise versions 10.9.0 and below may allows a remote attacker to view hidden field names in feature layers. This issue may reveal field names, but not not disclose features.	5.3	More Details
CVE-2021-40095	An issue was discovered in SquaredUp for SCOM 5.2.1.6654. The Download Log feature in System / Maintenance was susceptible to a local file inclusion vulnerability (when processing remote input in the log files downloaded by an authenticated administrator user), leading to the ability to read arbitrary files on the server filesystems.	4.9	More Details
CVE-2021-24714	The Import any XML or CSV File to WordPress plugin before 3.6.3 does not escape the Import's Title and Unique Identifier fields before outputting them in admin pages, which could allow high privilege users to perform Cross-Site attacks even when the unfiltered_html capability is disallowed.	4.8	More Details
CVE-2021-24718	The Contact Form, Survey & Popup Form Plugin for WordPress plugin before 1.5 does not properly sanitize some of its settings allowing high privilege users to perform Cross-Site Scripting attacks even when the unfiltered_html capability is disallowed	4.8	More Details
CVE-2015-20106	The ClickBank Affiliate Ads WordPress plugin through 1.20 does not escape its settings, allowing high privilege users to perform Cross-Site Scripting attacks even when the unfiltered_html is disallowed.	4.8	More Details
CVE-2021-25785	Taocms v2.5Beta5 was discovered to contain a cross-site scripting (XSS) vulnerability via the component Management column.	4.8	More Details
CVE-2021-35415	A stored cross-site scripting (XSS) vulnerability allows attackers to execute arbitrary web scripts or HTML via a crafted payload in the course "Title" and "Content" fields.	4.8	More Details
CVE-2021-29113	A remote file inclusion vulnerability in the ArcGIS Server help documentation may allow a remote, unauthenticated attacker to inject attacker supplied html into a page.	4.7	More Details
CVE-2021-43327	An issue was discovered on Renesas RX65 and RX65N devices. With a VCC glitch, an attacker can extract the security ID key from the device. Then, the protected firmware can be extracted.	4.6	More Details

CVE Number	Description	Base Score	Reference
CVE-2021-23261	Authenticated administrators may override the system configuration file and cause a denial of service.	4.5	More Details
CVE-2021-20862	Improper access control vulnerability in ELECOM routers (WRC-1167GST2 firmware v1.25 and prior, WRC-1167GST2A firmware v1.25 and prior, WRC-1167GST2H firmware v1.25 and prior, WRC-2533GS2-B firmware v1.52 and prior, WRC-2533GS2-W firmware v1.52 and prior, WRC-1750GS firmware v1.03 and prior, WRC-1750GSV firmware v2.11 and prior, WRC-1900GST firmware v1.03 and prior, WRC-2533GST firmware v1.03 and prior, WRC-2533GSTA firmware v1.03 and prior, WRC-2533GST2 firmware v1.25 and prior, WRC-2533GST2SP firmware v1.25 and prior, WRC-2533GST2-G firmware v1.25 and prior, and EDWRC-2533GST2 firmware v1.25 and prior) allows a network-adjacent unauthenticated attacker to bypass access restriction, and to obtain anti-CSRF tokens and change the product's settings via unspecified vectors.	4.3	More Details
CVE-2021-4015	firefly-iii is vulnerable to Cross-Site Request Forgery (CSRF)	4.3	More Details
CVE-2021-29863	IBM QRadar SIEM 7.3 and 7.4 is vulnerable to server side request forgery (SSRF). This may allow an authenticated attacker to send unauthorized requests from the system, potentially leading to network enumeration or facilitating other attacks. This vulnerability is due to an incomplete fix for CVE-2020-4786. IBM X-Force ID: 206087.	4.3	More Details
CVE-2021-4005	firefly-iii is vulnerable to Cross-Site Request Forgery (CSRF)	4.3	More Details
CVE-2021-43793	Discourse is an open source discussion platform. In affected versions a vulnerability in the Polls feature allowed users to vote multiple times in a single-option poll. The problem is patched in the latest tests-passed, beta and stable versions of Discourse	4.3	More Details
CVE-2021-43792	Discourse is an open source discussion platform. In affected versions a vulnerability affects users of tag groups who use the "Tags are visible only to the following groups" feature. A tag group may only allow a certain group (e.g. staff) to view certain tags. Users who were tracking or watching the tags via /preferences/tags, then have their staff status revoked will still see notifications related to the tag, but will not see the tag on each topic. This issue has been patched in stable version 2.7.11. Users are advised to upgrade as soon as possible.	4.3	More Details
CVE-2021-23562	This affects the package plupload before 2.3.9. A file name containing JavaScript code could be uploaded and run. An attacker would need to trick a user to upload this kind of file.	4.2	More Details

CVE Number	Description	Base Score	Reference
CVE-2021-23258	Authenticated users with Administrator or Developer roles may execute OS commands by SPEL Expression in Spring beans. SPEL Expression does not have security restrictions, which will cause attackers to execute arbitrary commands remotely (RCE).	4.2	More Details
CVE-2021-23259	Authenticated users with Administrator or Developer roles may execute OS commands by Groovy Script which uses Groovy lib to render a webpage. The groovy script does not have security restrictions, which will cause attackers to execute arbitrary commands remotely(RCE).	4.2	More Details
CVE-2020-27413	An issue was discovered in Mahavitaran android application 7.50 and below, allows local attackers to read cleartext username and password while the user is logged into the application.	4.2	More Details
CVE-2021-23262	Authenticated administrators may modify the main YAML configuration file and load a Java class resulting in RCE.	4.2	More Details
CVE-2021-37073	There is a Race Condition vulnerability in Huawei Smartphone.Successful exploitation of this vulnerability may lead to the detection result is tampered with.	3.7	More Details
CVE-2021-44185	Adobe Bridge version 11.1.2 (and earlier) and version 12.0 (and earlier) are affected by an out-of-bounds read vulnerability that could lead to disclosure of sensitive memory. An attacker could leverage this vulnerability to bypass mitigations such as ASLR. Exploitation of this issue requires user interaction in that a victim must open a malicious RGB file.	3.3	More Details
CVE-2021-44186	Adobe Bridge version 11.1.2 (and earlier) and version 12.0 (and earlier) are affected by an out-of-bounds read vulnerability that could lead to disclosure of sensitive memory. An attacker could leverage this vulnerability to bypass mitigations such as ASLR. Exploitation of this issue requires user interaction in that a victim must open a malicious SGI file.	3.3	More Details
CVE-2021-44187	Adobe Bridge version 11.1.2 (and earlier) and version 12.0 (and earlier) are affected by an out-of-bounds read vulnerability that could lead to disclosure of sensitive memory. An attacker could leverage this vulnerability to bypass mitigations such as ASLR. Exploitation of this issue requires user interaction in that a victim must open a malicious SGI file.	3.3	More Details
CVE-2021-39890	It was possible to bypass 2FA for LDAP users and access some specific pages with Basic Authentication in GitLab 14.1.1 and above.	3.1	More Details
CVE-2021-37298	Rejected reason: DO NOT USE THIS CANDIDATE NUMBER. ConsultIDs: none. Reason: This candidate was withdrawn by its CNA. Further investigation showed that it was not a security issue. Notes: none	N/A	More Details