SingCERT
Singapore Cyber Emergency Response Team

Security Bulletin 31 August 2022

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-2022-32548	An issue was discovered on certain DrayTek Vigor routers before July 2022 such as the Vigor3910 before 4.3.1.1. /cgi-bin/wlogin.cgi has a buffer overflow via the username or password to the aa or ab field.	10.0	More Details
CVE-2022-2234	An authenticated mySCADA myPRO 8.26.0 user may be able to modify parameters to run commands directly in the operating system.	9.9	More Details
CVE-2022-37057	D-Link Go-RT-AC750 GORTAC750_revA_v101b03 and GO-RT-AC750_revB_FWv200b02 are vulnerable to Command Injection via cgibin, ssdpcgi_main.	9.8	More Details
CVE-2022-36544	Edoc-doctor-appointment-system v1.0.1 was discovered to contain a SQL injection vulnerability via the id parameter at /patient/booking.php.	9.8	More Details

CVE Number	Description	Base Score	Reference
CVE-2022-36545	Edoc-doctor-appointment-system v1.0.1 was discovered to contain a SQL injection vulnerability via the id parameter at /patient/settings.php.	9.8	More Details
CVE-2022-38792	The exotel (aka exotel-py) package in PyPI as of 0.1.6 includes a code execution backdoor inserted by a third party.	9.8	More Details
CVE-2022-36755	D-Link DIR845L A1 contains a authentication vulnerability via an AUTHORIZED_GROUP=1 value, as demonstrated by a request for getcfg.php.	9.8	More Details
CVE-2022-36756	DIR845L A1 v1.00-v1.03 is vulnerable to command injection via /htdocs/upnpinc/gena.php.	9.8	More Details
CVE-2022-37053	TRENDnet TEW733GR v1.03B01 is vulnerable to Command injection via /htdocs/upnpinc/gena.php.	9.8	More Details
CVE-2022-38078	Movable Type XMLRPC API provided by Six Apart Ltd. contains a command injection vulnerability. Sending a specially crafted message by POST method to Movable Type XMLRPC API may allow arbitrary Perl script execution, and an arbitrary OS command may be executed through it. Affected products and versions are as follows: Movable Type 7 r.5202 and earlier, Movable Type Advanced 7 r.5202 and earlier, Movable Type 6.8.6 and earlier, Movable Type Advanced 6.8.6 and earlier, Movable Type Premium 1.52 and earlier, and Movable Type Premium Advanced 1.52 and earlier. Note that all versions of Movable Type 4.0 or later including unsupported (End-of-Life, EOL) versions are also affected by this vulnerability.	9.8	More Details
CVE-2022-37152	An issue was discovered in Online Diagnostic Lab Management System 1.0, There is a SQL injection vulnerability via "dob" parameter in "/classes/Users.php?f=save_client"	9.8	More Details
CVE-2022-38556	Trendnet TEW733GR v1.03B01 contains a Static Default Credential vulnerability in /etc/init0.d/S80telnetd.sh.	9.8	More Details
CVE-2022-38557	D-Link DIR845L v1.00-v1.03 contains a Static Default Credential vulnerability in /etc/init0.d/S80telnetd.sh.	9.8	More Details

CVE Number	Description	Base Score	Reference
CVE-2022-37055	D-Link Go-RT-AC750 GORTAC750_revA_v101b03 and GO-RT-AC750_revB_FWv200b02 are vulnerable to Buffer Overflow via cgibin, hnap_main,	9.8	More Details
CVE-2022-37056	D-Link GO-RT-AC750 GORTAC750_revA_v101b03 and GO-RT-AC750_revB_FWv200b02 is vulnerable to Command Injection via /cgibin, hnap_main,	9.8	More Details
CVE-2022-38555	Linksys E1200 v1.0.04 is vulnerable to Buffer Overflow via ej_get_web_page_name.	9.8	More Details
CVE-2022-36543	Edoc-doctor-appointment-system v1.0.1 was discovered to contain a SQL injection vulnerability via the id parameter at /patient/doctors.php.	9.8	More Details
CVE-2022-36683	Simple Task Scheduling System v1.0 was discovered to contain a SQL injection vulnerability via the id parameter at /classes/Master.php?f=delete_payment.	9.8	More Details
CVE-2022-36706	Ingredients Stock Management System v1.0 was discovered to contain a SQL injection vulnerability via the Id parameter at /stocks/manage_stockout.php.	9.8	More Details
CVE-2022-36682	Simple Task Scheduling System v1.0 was discovered to contain a SQL injection vulnerability via the id parameter at /classes/Master.php?f=delete_student.	9.8	More Details
CVE-2022-36681	Simple Task Scheduling System v1.0 was discovered to contain a SQL injection vulnerability via the id parameter at /classes/Master.php?f=delete_account.	9.8	More Details
CVE-2022-36680	Simple Task Scheduling System v1.0 was discovered to contain a SQL injection vulnerability via the id parameter at /classes/Master.php?f=delete_schedule.	9.8	More Details
CVE-2022-36679	Simple Task Scheduling System v1.0 was discovered to contain a SQL injection vulnerability via the id parameter at /admin/?page=user/manage_user.	9.8	More Details
CVE-2022-36678	Simple Task Scheduling System v1.0 was discovered to contain a SQL injection vulnerability via the id parameter at /classes/Master.php?f=delete_category.	9.8	More Details

CVE Number	Description	Base Score	Reference
CVE-2022-31499	Nortek Linear eMerge E3-Series devices before 0.32-08f allow an unauthenticated attacker to inject OS commands via ReaderNo. NOTE: this issue exists because of an incomplete fix for CVE-2019-7256.	9.8	More Details
CVE-2022-28747	Key reuse in GoSecure Titan Inbox Detection & Response (IDR) through 2022-04-05 leads to remote code execution. To exploit this vulnerability, an attacker must craft and sign a serialized payload.	9.8	More Details
CVE-2022-36719	Library Management System v1.0 was discovered to contain a SQL injection vulnerability via the ok parameter at /admin/history.php.	9.8	More Details
CVE-2022-36716	Library Management System v1.0 was discovered to contain a SQL injection vulnerability via the id parameter at /admin/changestock.php.	9.8	More Details
CVE-2022-36715	Library Management System v1.0 was discovered to contain a SQL injection vulnerability via the name parameter at /admin/search.php.	9.8	More Details
CVE-2022-36697	Ingredients Stock Management System v1.0 was discovered to contain a SQL injection vulnerability via the id parameter at /classes/Master.php?f=delete_waste.	9.8	More Details
CVE-2022-36696	Ingredients Stock Management System v1.0 was discovered to contain a SQL injection vulnerability via the id parameter at /classes/Master.php?f=delete_stockout.	9.8	More Details
CVE-2022-36695	Ingredients Stock Management System v1.0 was discovered to contain a SQL injection vulnerability via the id parameter at /classes/Master.php?f=delete_stockin.	9.8	More Details
CVE-2022-36705	Ingredients Stock Management System v1.0 was discovered to contain a SQL injection vulnerability via the Id parameter at /stocks/manage_waste.php.	9.8	More Details
CVE-2022-36708	Library Management System v1.0 was discovered to contain a SQL injection vulnerability via the Id parameter at /student/bookdetails.php.	9.8	More Details
CVE-2021-39815	The PowerVR GPU driver allows unprivileged apps to allocated pinned memory, unpin it (which makes it available to be freed), and continue using the page in GPU calls. No privileges required and this results in kernel memory corruption.Product: AndroidVersions: Android SoCAndroid ID: A-232440670	9.8	More Details

CVE Number	Description	Base Score	Reference
CVE-2022-36572	Sinsiu Sinsiu Enterprise Website System v1.1.1.0 was discovered to contain a remote code execution (RCE) vulnerability via the component /upload/admin.php?/deal/.	9.8	More Details
CVE-2022-36735	Library Management System v1.0 was discovered to contain a SQL injection vulnerability via the bookId parameter at /admin/delete.php.	9.8	More Details
CVE-2022-36734	Library Management System v1.0 was discovered to contain a SQL injection vulnerability via the RollNo parameter at /admin/delstu.php.	9.8	More Details
CVE-2022-36733	Library Management System v1.0 was discovered to contain a SQL injection vulnerability via the M_Id parameter at /admin/del.php.	9.8	More Details
CVE-2022-36732	Library Management System v1.0 was discovered to contain a SQL injection vulnerability via the id parameter at /librarian/dele.php.	9.8	More Details
CVE-2022-36731	Library Management System v1.0 was discovered to contain a SQL injection vulnerability via the RollNo parameter at /librarian/delstu.php.	9.8	More Details
CVE-2022-36730	Library Management System v1.0 was discovered to contain a SQL injection vulnerability via the bookId parameter at /librarian/delete.php.	9.8	More Details
CVE-2022-37176	Tenda AC6(AC1200) v5.0 Firmware v02.03.01.114 and below contains a vulnerability which allows attackers to remove the Wi-Fi password and force the device into open security mode via a crafted packet sent to goform/setWizard.	9.8	More Details
CVE-2022-37149	WAVLINK WL-WN575A3 RPT75A3.V4300.201217 was discovered to contain a command injection vulnerability when operating the file adm.cgi. This vulnerability allows attackers to execute arbitrary commands via the username parameter.	9.8	More Details
CVE-2022-38116	Le-yan Personnel and Salary Management System has hard-coded database account and password within the website source code. An unauthenticated remote attacker can access, modify system data or disrupt service.	9.8	More Details
CVE-2022-36714	Library Management System v1.0 was discovered to contain a SQL injection vulnerability via the Section parameter at /staff/lab.php.	9.8	More Details

CVE Number	Description	Base Score	Reference
CVE-2022-36713	Library Management System v1.0 was discovered to contain a SQL injection vulnerability via the Section parameter at /librarian/lab.php.	9.8	More Details
CVE-2022-36712	Library Management System v1.0 was discovered to contain a SQL injection vulnerability via the id parameter at /staff/studentdetails.php.	9.8	More Details
CVE-2022-36711	Library Management System v1.0 was discovered to contain a SQL injection vulnerability via the id parameter at /staff/bookdetails.php.	9.8	More Details
CVE-2022-36709	Library Management System v1.0 was discovered to contain a SQL injection vulnerability via the id parameter at /staff/edit_book_details.php.	9.8	More Details
CVE-2022-36560	Seiko SkyBridge MB-A200 v01.00.04 and below was discovered to contain multiple hard-coded passcodes for root. Attackers are able to access the passcodes at /etc/srapi/config/system.conf and /usr/sbin/ssol-sshd.sh.	9.8	More Details
CVE-2022-36559	Seiko SkyBridge MB-A200 v01.00.04 and below was discovered to contain a command injection vulnerability via the Ping parameter at ping_exec.cgi.	9.8	More Details
CVE-2022-36558	Seiko SkyBridge MB-A100/A110 v4.2.0 and below implements a hard-coded passcode for the root account. Attackers are able to access the passcord via the file /etc/ciel.cfg.	9.8	More Details
CVE-2022-36557	Seiko SkyBridge MB-A100/A110 v4.2.0 and below was discovered to contain an arbitrary file upload vulnerability via the restore backup function. This vulnerability allows attackers to execute arbitrary code via a crafted html file.	9.8	More Details
CVE-2022-36556	Seiko SkyBridge MB-A100/A110 v4.2.0 and below was discovered to contain a command injection vulnerability via the ipAddress parameter at 07system08execute_ping_01.	9.8	More Details
CVE-2022-36555	Hytec Inter HWL-2511-SS v1.05 and below implements a SHA512crypt hash for the root account which can be easily cracked via a brute-force attack.	9.8	More Details
CVE-2022-36554	A command injection vulnerability in the CLI (Command Line Interface) implementation of Hytec Inter HWL-2511-SS v1.05 and below allows attackers to execute arbitrary commands with root privileges.	9.8	More Details

CVE Number	Description	Base Score	Reference
CVE-2022-36553	Hytec Inter HWL-2511-SS v1.05 and below was discovered to contain a command injection vulnerability via the component /www/cgi-bin/popen.cgi.	9.8	More Details
CVE-2022-32993	TOTOLINK A7000R V4.1cu.4134 was discovered to contain an access control issue via /cgi-bin/ExportSettings.sh.	9.8	More Details
CVE-2022-22897	A SQL injection vulnerability in the product_all_one_img and image_product parameters of the ApolloTheme AP PageBuilder component through 2.4.4 for PrestaShop allows unauthenticated attackers to exfiltrate database data.	9.8	More Details
CVE-2022-25644	All versions of package @pendo324/get-process-by-name are vulnerable to Arbitrary Code Execution due to improper sanitization of getProcessByName function.	9.8	More Details
CVE-2022-21165	All versions of package font-converter are vulnerable to Arbitrary Command Injection due to missing sanitization of input that potentially flows into the child_process.exec() function.	9.8	More Details
CVE-2022-34668	NVFLARE, versions prior to 2.1.4, contains a vulnerability that deserialization of Untrusted Data due to Pickle usage may allow an unprivileged network attacker to cause Remote Code Execution, Denial Of Service, and Impact to both Confidentiality and Integrity.	9.8	More Details
CVE-2022-36693	Ingredients Stock Management System v1.0 was discovered to contain a SQL injection vulnerability via the id parameter at /classes/Master.php?f=delete_item.	9.8	More Details
CVE-2022-36692	Ingredients Stock Management System v1.0 was discovered to contain a SQL injection vulnerability via the id parameter at /classes/Master.php?f=delete_category.	9.8	More Details
CVE-2021-43329	A SQL injection vulnerability in license_update.php in Mumara Classic through 2.93 allows a remote unauthenticated attacker to execute arbitrary SQL commands via the license parameter.	9.8	More Details
CVE-2022-37067	H3C GR-1200W MiniGRW1A0V100R006 was discovered to contain a stack overflow via the function UpdateWanParamsMulti.	9.8	More Details
CVE-2022-37091	H3C H200 H200V100R004 was discovered to contain a stack overflow via the function EditWlanMacList.	9.8	More Details

CVE Number	Description	Base Score	Reference
CVE-2022-37090	H3C H200 H200V100R004 was discovered to contain a stack overflow via the function Edit_BasicSSID.	9.8	More Details
CVE-2022-37089	H3C H200 H200V100R004 was discovered to contain a stack overflow via the function EditMacList.	9.8	More Details
CVE-2022-37088	H3C H200 H200V100R004 was discovered to contain a stack overflow via the function SetAP5GWifiById.	9.8	More Details
CVE-2022-37087	H3C H200 H200V100R004 was discovered to contain a stack overflow via the function SetMobileAPInfoById.	9.8	More Details
CVE-2022-37086	H3C H200 H200V100R004 was discovered to contain a stack overflow via the function Asp_SetTimingtimeWifiAndLed.	9.8	More Details
CVE-2022-37085	H3C H200 H200V100R004 was discovered to contain a stack overflow via the AddWlanMacList function.	9.8	More Details
CVE-2022-37073	H3C GR-1200W MiniGRW1A0V100R006 was discovered to contain a stack overflow via the function UpdateWanModeMulti.	9.8	More Details
CVE-2022-37072	H3C GR-1200W MiniGRW1A0V100R006 was discovered to contain a stack overflow via the function UpdateWanLinkspyMulti.	9.8	More Details
CVE-2022-37071	H3C GR-1200W MiniGRW1A0V100R006 was discovered to contain a stack overflow via the function UpdateOne2One.	9.8	More Details
CVE-2022-37070	H3C GR-1200W MiniGRW1A0V100R006 was discovered to contain a command injection vulnerability via the param parameter at DelL2tpLNSList.	9.8	More Details
CVE-2022-37069	H3C GR-1200W MiniGRW1A0V100R006 was discovered to contain a stack overflow via the function UpdateSnat.	9.8	More Details
CVE-2022-37068	H3C GR-1200W MiniGRW1A0V100R006 was discovered to contain a stack overflow via the function UpdateMacCloneFinal.	9.8	More Details

CVE Number	Description	Base Score	Reference
CVE-2022-37066	H3C GR-1200W MiniGRW1A0V100R006 was discovered to contain a stack overflow via the function UpdateDDNS.	9.8	More Details
CVE-2022-37093	H3C H200 H200V100R004 was discovered to contain a stack overflow via the function AddMacList.	9.8	More Details
CVE-2022-36520	H3C GR-1200W MiniGRW1A0V100R006 was discovered to contain a stack overflow via the function DEleteusergroup.	9.8	More Details
CVE-2022-36519	H3C GR-1200W MiniGRW1A0V100R006 was discovered to contain a stack overflow via the function AddWlanMacList.	9.8	More Details
CVE-2022-36518	H3C GR-1200W MiniGRW1A0V100R006 was discovered to contain a stack overflow via the function EditWlanMacList.	9.8	More Details
CVE-2022-36517	H3C GR-1200W MiniGRW1A0V100R006 was discovered to contain a stack overflow via the function debug_wlan_advance.	9.8	More Details
CVE-2022-36516	H3C GR-1200W MiniGRW1A0V100R006 was discovered to contain a stack overflow via the function ap_version_check.	9.8	More Details
CVE-2022-36515	H3C GR-1200W MiniGRW1A0V100R006 was discovered to contain a stack overflow via the function addactionlist.	9.8	More Details
CVE-2022-36514	H3C GR-1200W MiniGRW1A0V100R006 was discovered to contain a stack overflow via the function WanModeSetMultiWan.	9.8	More Details
CVE-2022-36513	H3C GR-1200W MiniGRW1A0V100R006 was discovered to contain a stack overflow via the function edditactionlist.	9.8	More Details
CVE-2022-36511	H3C GR-1200W MiniGRW1A0V100R006 was discovered to contain a stack overflow via the function EditApAdvanceInfo.	9.8	More Details

CVE Number	Description	Base Score	Reference
CVE-2022-34960	The container package in MikroTik RouterOS 7.4beta4 allows an attacker to create mount points pointing to symbolic links, which resolve to locations on the host device. This allows the attacker to mount any arbitrary file to any location on the host.	9.8	More Details
CVE-2022-32839	The issue was addressed with improved bounds checks. This issue is fixed in macOS Monterey 12.5, macOS Big Sur 11.6.8, Security Update 2022-005 Catalina, iOS 15.6 and iPadOS 15.6, tvOS 15.6, watchOS 8.7. A remote user may cause an unexpected app termination or arbitrary code execution.	9.8	More Details
CVE-2022-37181	72crm 9.0 has an Arbitrary file upload vulnerability.	9.8	More Details
CVE-2022-20122	The PowerVR GPU driver allows unprivileged apps to allocated pinned memory, unpin it (which makes it available to be freed), and continue using the page in GPU calls. No privileges required and this results in kernel memory corruption.Product: AndroidVersions: Android SoCAndroid ID: A-232441339	9.8	More Details
CVE-2022-37092	H3C H200 H200V100R004 was discovered to contain a stack overflow via the function SetAPWifiorLedInfoById.	9.8	More Details
CVE-2022-37094	H3C H200 H200V100R004 was discovered to contain a stack overflow via the function Edit_BasicSSID_5G.	9.8	More Details
CVE-2022-37159	Claroline 13.5.7 and prior is vulnerable to Remote code execution via arbitrary file upload.	9.8	More Details
CVE-2022-37804	Tenda AC1206 V15.03.06.23 was discovered to contain a stack overflow via the time parameter in the function saveParentControlInfo.	9.8	More Details
CVE-2022-37158	RuoYi v3.8.3 has a Weak password vulnerability in the management system.	9.8	More Details
CVE-2022-37816	Tenda AC1206 V15.03.06.23 was discovered to contain a stack overflow via the function fromSetIpMacBind.	9.8	More Details

CVE Number	Description	Base Score	Reference
CVE-2022-37815	Tenda AC1206 V15.03.06.23 was discovered to contain a stack overflow via the PPPOEPassword parameter in the function formQuickIndex.	9.8	More Details
CVE-2022-37814	Tenda AC1206 V15.03.06.23 was discovered to contain multiple stack overflows via the deviceMac and the device_id parameters in the function addWifiMacFilter.	9.8	More Details
CVE-2022-37813	Tenda AC1206 V15.03.06.23 was discovered to contain a stack overflow via the function fromSetSysTime.	9.8	More Details
CVE-2022-37812	Tenda AC1206 V15.03.06.23 was discovered to contain a stack overflow via the firewallEn parameter in the function formSetFirewallCfg.	9.8	More Details
CVE-2022-37811	Tenda AC1206 V15.03.06.23 was discovered to contain a stack overflow via the startIp parameter in the function formSetPPTPServer.	9.8	More Details
CVE-2022-37810	Tenda AC1206 V15.03.06.23 was discovered to contain a command injection vulnerability via the mac parameter in the function formWriteFacMac.	9.8	More Details
CVE-2022-37809	Tenda AC1206 V15.03.06.23 was discovered to contain a stack overflow via the speed_dir parameter in the function formSetSpeedWan.	9.8	More Details
CVE-2022-37808	Tenda AC1206 V15.03.06.23 was discovered to contain a stack overflow via the index parameter in the function formWifiWpsOOB.	9.8	More Details
CVE-2022-37807	Tenda AC1206 V15.03.06.23 was discovered to contain a stack overflow via the function formSetClientState.	9.8	More Details
CVE-2022-37806	Tenda AC1206 V15.03.06.23 was discovered to contain a stack overflow via the page parameter in the function fromDhcpListClient.	9.8	More Details
CVE-2022-37805	Tenda AC1206 V15.03.06.23 was discovered to contain a stack overflow via the function fromWizardHandle.	9.8	More Details

CVE Number	Description	Base Score	Reference
CVE-2022-37803	Tenda AC1206 V15.03.06.23 was discovered to contain a stack overflow via the page parameter in the function fromAddressNat.	9.8	More Details
CVE-2022-37095	H3C H200 H200V100R004 was discovered to contain a stack overflow via the function UpdateWanParams.	9.8	More Details
CVE-2022-37802	Tenda AC1206 V15.03.06.23 was discovered to contain a stack overflow via the page parameter in the function fromNatStaticSetting.	9.8	More Details
CVE-2022-37801	Tenda AC1206 V15.03.06.23 was discovered to contain a stack overflow via the list parameter at the function formSetQosBand.	9.8	More Details
CVE-2022-37800	Tenda AC1206 V15.03.06.23 was discovered to contain a stack overflow via the list parameter at the function fromSetRouteStatic.	9.8	More Details
CVE-2022-37799	Tenda AC1206 V15.03.06.23 was discovered to contain a stack overflow via the time parameter at the function setSmartPowerManagement.	9.8	More Details
CVE-2022-37798	Tenda AC1206 V15.03.06.23 was discovered to contain a stack overflow via the list parameter at the function formSetVirtualSer.	9.8	More Details
CVE-2022-37242	MDaemon Technologies SecurityGateway for Email Servers 8.5.2, is vulnerable to HTTP Response splitting via the data parameter.	9.8	More Details
CVE-2022-37240	MDaemon Technologies SecurityGateway for Email Servers 8.5.2 is vulnerable to HTTP Response splitting via the format parameter.	9.8	More Details
CVE-2022-37100	H3C H200 H200V100R004 was discovered to contain a stack overflow via the function UpdateMacClone.	9.8	More Details
CVE-2022-37099	H3C H200 H200V100R004 was discovered to contain a stack overflow via the function UpdateSnat.	9.8	More Details
CVE-2022-37098	H3C H200 H200V100R004 was discovered to contain a stack overflow via the function UpdateIpv6Params.	9.8	More Details

CVE Number	Description	Base Score	Reference
CVE-2022-37097	H3C H200 H200V100R004 was discovered to contain a stack overflow via the function SetAPInfoById.	9.8	More Details
CVE-2022-37096	H3C H200 H200V100R004 was discovered to contain a stack overflow via the function EnableIpv6.	9.8	More Details
CVE-2022-36749	RPi-Jukebox-RFID v2.3.0 was discovered to contain a command injection vulnerability via the component /htdocs/utils/Files.php. This vulnerability is exploited via a crafted payload injected into the file name of an uploaded file.	9.8	More Details
CVE-2019-15167	The VRRP parser in tcpdump before 4.9.3 has a buffer over-read in print-vrrp.c:vrrp_print() for VRRP version 3, a different vulnerability than CVE-2018-14463.	9.1	More Details

OTHER VULNERABILITIES

CVE Number	Description	Base Score	Reference
CVE-2022-2031	A flaw was found in Samba. The security vulnerability occurs when KDC and the kpasswd service share a single account and set of keys, allowing them to decrypt each other's tickets. A user who has been requested to change their password, can exploit this flaw to obtain and use tickets to other services.	8.8	More Details
CVE-2022-20824	A vulnerability in the Cisco Discovery Protocol feature of Cisco FXOS Software and Cisco NX-OS Software could allow an unauthenticated, adjacent attacker to execute arbitrary code with root privileges or cause a denial of service (DoS) condition on an affected device. This vulnerability is due to improper input validation of specific values that are within a Cisco Discovery Protocol message. An attacker could exploit this vulnerability by sending a malicious Cisco Discovery Protocol packet to an affected device. A successful exploit could allow the attacker to execute arbitrary code with root privileges or cause the Cisco Discovery Protocol process to crash and restart multiple times, which would cause the affected device to reload, resulting in a DoS condition. Note: Cisco Discovery Protocol is a Layer 2 protocol. To exploit this vulnerability, an attacker must be in the same broadcast domain as the affected device (Layer 2 adjacent).	8.8	More Details

CVE Number	Description	Base Score	Reference
CVE-2022-36700	Ingredients Stock Management System v1.0 was discovered to contain a SQL injection vulnerability via the id parameter at /items/manage_item.php.	8.8	More Details
CVE-2021-25642	ZKConfigurationStore which is optionally used by CapacityScheduler of Apache Hadoop YARN deserializes data obtained from ZooKeeper without validation. An attacker having access to ZooKeeper can run arbitrary commands as YARN user by exploiting this. Users should upgrade to Apache Hadoop 2.10.2, 3.2.4, 3.3.4 or later (containing YARN-11126) if ZKConfigurationStore is used.	8.8	More Details
CVE-2022-36804	Multiple API endpoints in Atlassian Bitbucket Server and Data Center 7.0.0 before version 7.6.17, from version 7.7.0 before version 7.17.10, from version 7.18.0 before version 7.21.4, from version 8.0.0 before version 8.0.3, from version 8.1.0 before version 8.1.3, and from version 8.2.0 before version 8.2.2, and from version 8.3.0 before 8.3.1 allows remote attackers with read permissions to a public or private Bitbucket repository to execute arbitrary code by sending a malicious HTTP request. This vulnerability was reported via our Bug Bounty Program by TheGrandPew.	8.8	More Details
CVE-2022-38118	OAKlouds Portal website's Meeting Room has insufficient validation for user input. A remote attacker with general user privilege can perform SQL-injection to access, modify, delete database, perform system operations and disrupt service.	8.8	More Details
CVE-2022-0336	The Samba AD DC includes checks when adding service principals names (SPNs) to an account to ensure that SPNs do not alias with those already in the database. Some of these checks are able to be bypassed if an account modification re-adds an SPN that was previously present on that account, such as one added when a computer is joined to a domain. An attacker who has the ability to write to an account can exploit this to perform a denial-of-service attack by adding an SPN that matches an existing service. Additionally, an attacker who can intercept traffic can impersonate existing services, resulting in a loss of confidentiality and integrity.	8.8	More Details
CVE-2022-32427	PrinterLogic Windows Client through 25.0.0.676 allows attackers to execute directory traversal. Authenticated users with prior knowledge of the driver filename could exploit this to escalate privileges or distribute malicious content. This issue has been resolved in PrinterLogic Windows Client 25.0.0688 and all affected are advised to upgrade.	8.8	More Details

CVE Number	Description	Base Score	Reference
CVE-2022-20921	A vulnerability in the API implementation of Cisco ACI Multi-Site Orchestrator (MSO) could allow an authenticated, remote attacker to elevate privileges on an affected device. This vulnerability is due to improper authorization on specific APIs. An attacker could exploit this vulnerability by sending crafted HTTP requests. A successful exploit could allow an attacker who is authenticated with non-Administrator privileges to elevate to Administrator privileges on an affected device.	8.8	More Details
CVE-2021-4112	A flaw was found in ansible-tower where the default installation is vulnerable to job isolation escape. This flaw allows an attacker to elevate the privilege from a low privileged user to an AWX user from outside the isolated environment.	8.8	More Details
CVE-2022-32893	An out-of-bounds write issue was addressed with improved bounds checking. This issue is fixed in iOS 15.6.1 and iPadOS 15.6.1, macOS Monterey 12.5.1, Safari 15.6.1. Processing maliciously crafted web content may lead to arbitrary code execution. Apple is aware of a report that this issue may have been actively exploited.	8.8	More Details
CVE-2022-36699	Ingredients Stock Management System v1.0 was discovered to contain a SQL injection vulnerability via the id parameter at /categories/manage_category.php.	8.8	More Details
CVE-2022-36703	Ingredients Stock Management System v1.0 was discovered to contain a SQL injection vulnerability via the id parameter at /stocks/manage_stockin.php.	8.8	More Details
CVE-2022-3019	The forgot password token basically just makes us capable of taking over the account of whoever comment in an app that we can see (bruteforcing comment id's might also be an option but I wouldn't count on it, since it would take a long time to find a valid one).	8.8	More Details
CVE-2022-36686	Ingredients Stock Management System v1.0 was discovered to contain a SQL injection vulnerability via the month parameter at /admin/?page=reports/stockin&month=.	8.8	More Details
CVE-2022-36690	Ingredients Stock Management System v1.0 was discovered to contain a SQL injection vulnerability via the id parameter at /admin/?page=user/manage_user&id=.	8.8	More Details
CVE-2022-38772	Zoho ManageEngine OpManager, OpManager Plus, OpManager MSP, Network Configuration Manager, NetFlow Analyzer, and OpUtils before 125658, 126003, 126105, and 126120 allow authenticated users to make database changes that lead to remote code execution in the NMAP feature.	8.8	More Details

CVE Number	Description	Base Score	Reference
CVE-2022-38625	Patlite NH-FB v1.46 and below was discovered to contain insufficient firmware validation during the upgrade firmware file upload process. This vulnerability allows authenticated attackers to create and upload their own custom-built firmware and inject malicious code. NOTE: the vendor's position is that this is a design choice, not a vulnerability	8.8	More Details
CVE-2022-36698	Ingredients Stock Management System v1.0 was discovered to contain a SQL injection vulnerability via the id parameter at /categories/view_category.php.	8.8	More Details
CVE-2022-37178	An issue was discovered in 72crm 9.0. There is a SQL Injection vulnerability in View the task calendar.	8.8	More Details
CVE-2022-32744	A flaw was found in Samba. The KDC accepts kpasswd requests encrypted with any key known to it. By encrypting forged kpasswd requests with its own key, a user can change other users' passwords, enabling full domain takeover.	8.8	More Details
CVE-2022-36688	Ingredients Stock Management System v1.0 was discovered to contain a SQL injection vulnerability via the month parameter at /admin/?page=reports/stockout&month=.	8.8	More Details
CVE-2022-36701	Ingredients Stock Management System v1.0 was discovered to contain a SQL injection vulnerability via the id parameter at /items/view_item.php.	8.8	More Details
CVE-2022-36546	Edoc-doctor-appointment-system v1.0.1 was discovered to contain a Cross-Site Request Forgery (CSRF) via /patient/settings.php.	8.8	More Details
CVE-2022-36563	Incorrect access control in the install directory (C:\RailsInstaller) of Rubyinstaller2 v3.1.2 and below allows authenticated attackers to execute arbitrary code via overwriting binaries located in the directory.	8.8	More Details
CVE-2022-34375	Dell Container Storage Modules 1.2 contains a path traversal vulnerability in goiscsi and gobrick libraries. A remote authenticated malicious user with low privileges could exploit this vulnerability leading to unintentional access to path outside of restricted directory.	8.8	More Details
CVE-2022-31773	IBM DataPower Gateway V10CD, 10.0.1, and 2018.4.1 is vulnerable to cross-site request forgery which could allow an attacker to execute malicious and unauthorized actions transmitted from a user that the website trusts. IBM X-Force ID: 228357.	8.8	More Details

CVE Number	Description	Base Score	Reference
CVE-2021-3020	An issue was discovered in ClusterLabs Hawk (aka HA Web Konsole) through 2.3.0-15. It ships the binary hawk_invoke (built from tools/hawk_invoke.c), intended to be used as a setuid program. This allows the hacluster user to invoke certain commands as root (with an attempt to limit this to safe combinations). This user is able to execute an interactive "shell" that isn't limited to the commands specified in hawk_invoke, allowing escalation to root.	8.8	More Details
CVE-2022-25625	A malicious unauthorized PAM user can access the administration configuration data and change the values.	8.8	More Details
CVE-2022-37333	SQL injection vulnerability in the Exment ((PHP8) exceedone/exment v5.0.2 and earlier and exceedone/laravel-admin v3.0.0 and earlier, (PHP7) exceedone/exment v4.4.2 and earlier and exceedone/laravel-admin v2.2.2 and earlier) allows remote authenticated attackers to execute arbitrary SQL commands.	8.8	More Details
CVE-2022-36565	Incorrect access control in the install directory (C:\Wamp64) of Wamp v3.2.6 and below allows authenticated attackers to execute arbitrary code via overwriting binaries located in the directory.	8.8	More Details
CVE-2022-36119	An issue was discovered in Blue Prism Enterprise 6.0 through 7.01. In a misconfigured environment that exposes the Blue Prism Application server, it is possible for a domain authenticated user to send a crafted message to the Blue Prism Server and accomplish a remote code execution attack that is possible because of insecure deserialization. Exploitation of this vulnerability allows for code to be executed in the context of the Blue Prism Server service.	8.8	More Details
CVE-2022-36564	Incorrect access control in the install directory (C:\Strawberry) of StrawberryPerl v5.32.1.1 and below allows authenticated attackers to execute arbitrary code via overwriting binaries located in the directory.	8.8	More Details
CVE-2022-36633	Teleport 9.3.6 is vulnerable to Command injection leading to Remote Code Execution. An attacker can craft a malicious ssh agent installation link by URL encoding a bash escape with carriage return line feed. This url encoded payload can be used in place of a token and sent to a user in a social engineering attack. This is fully unauthenticated attack utilizing the trusted teleport server to deliver the payload.	8.8	More Details
CVE-2022-36562	Incorrect access control in the install directory (C:\Ruby31-x64) of Rubyinstaller2 v3.1.2 and below allows authenticated attackers to execute arbitrary code via overwriting binaries located in the directory.	8.8	More Details

CVE Number	Description	Base Score	Reference
CVE-2022-36689	Ingredients Stock Management System v1.0 was discovered to contain a SQL injection vulnerability via the month parameter at /admin/?page=reports/waste&month=.	8.8	More Details
CVE-2022-36529	Kensite CMS v1.0 was discovered to contain multiple SQL injection vulnerabilities via the name and oldname parameters at /framework/mod/db/DBMapper.xml.	8.8	More Details
CVE-2022-1043	A flaw was found in the Linux kernel's io_uring implementation. This flaw allows an attacker with a local account to corrupt system memory, crash the system or escalate privileges.	8.8	More Details
CVE-2022-34374	Dell Container Storage Modules 1.2 contains an OS command injection in goiscsi and gobrick libraries. A remote authenticated malicious user with low privileges could exploit this vulnerability leading to to execute arbitrary OS commands on the affected system.	8.8	More Details
CVE-2022-2915	A Heap-based Buffer Overflow vulnerability in the SonicWall SMA100 appliance allows a remote authenticated attacker to cause Denial of Service (DoS) on the appliance or potentially lead to code execution. This vulnerability impacts 10.2.1.5-34sv and earlier versions.	8.8	More Details
CVE-2022-36704	Library Management System v1.0 was discovered to contain a SQL injection vulnerability via the Id parameter at /librarian/studentdetails.php.	8.8	More Details
CVE-2022-36721	Library Management System v1.0 was discovered to contain a SQL injection vulnerability via the Textbook parameter at /admin/modify.php.	8.8	More Details
CVE-2022-36720	Library Management System v1.0 was discovered to contain a SQL injection vulnerability via the id parameter at /admin/modify1.php.	8.8	More Details
CVE-2022-2465	Rockwell Automation ISaGRAF Workbench software versions 6.0 through 6.6.9 are affected by a Deserialization of Untrusted Data vulnerability. ISaGRAF Workbench does not limit the objects that can be deserialized. This vulnerability allows attackers to craft a malicious serialized object that, if opened by a local user in ISaGRAF Workbench, may result in remote code execution. This vulnerability requires user interaction to be successfully exploited.	8.6	More Details

CVE Number	Description	Base Score	Reference
CVE-2022-20823	A vulnerability in the OSPF version 3 (OSPFv3) feature of Cisco NX-OS Software could allow an unauthenticated, remote attacker to cause a denial of service (DoS) condition on an affected device. This vulnerability is due to incomplete input validation of specific OSPFv3 packets. An attacker could exploit this vulnerability by sending a malicious OSPFv3 link-state advertisement (LSA) to an affected device. A successful exploit could allow the attacker to cause the OSPFv3 process to crash and restart multiple times, causing the affected device to reload and resulting in a DoS condition. Note: The OSPFv3 feature is disabled by default. To exploit this vulnerability, an attacker must be able to establish a full OSPFv3 neighbor state with an affected device. For more information about exploitation conditions, see the Details section of this advisory.	8.6	More Details
CVE-2022-31232	SmartFabric storage software version 1.0.0 contains a Command-Injection vulnerability. A remote unauthenticated attacker may potentially exploit this vulnerability to gain access and perform actions on the affected system.	8.6	More Details
CVE-2022-1117	A vulnerability was found in fapolicyd. The vulnerability occurs due to an assumption on how glibc names the runtime linker, a build time regular expression may not correctly detect the runtime linker. The consequence is that the pattern detection for applications launched by the run time linker may fail to detect the pattern and allow execution.	8.4	More Details
CVE-2022-27546	HCL iNotes is susceptible to a Reflected Cross-site Scripting (XSS) vulnerability caused by improper validation of user-supplied input supplied with a form POST request. A remote attacker could exploit this vulnerability using a specially-crafted URL to execute script in a victim's web browser within the security context of the hosting web site and/or steal the victim's cookie-based authentication credentials.	8.3	More Details
CVE-2021-3929	A DMA reentrancy issue was found in the NVM Express Controller (NVME) emulation in QEMU. This CVE is similar to CVE-2021-3750 and, just like it, when the reentrancy write triggers the reset function nvme_ctrl_reset(), data structs will be freed leading to a use-after-free issue. A malicious guest could use this flaw to crash the QEMU process on the host, resulting in a denial of service condition or, potentially, executing arbitrary code within the context of the QEMU process on the host.	8.2	More Details
CVE-2022-31269	Nortek Linear eMerge E3-Series devices through 0.32-09c place admin credentials in /test.txt that allow an attacker to open a building's doors. (This occurs in situations where the CVE-2019-7271 default credentials have been changed.)	8.2	More Details

CVE Number	Description	Base Score	Reference
CVE-2022-38132	Command injection vulnerability in Linksys MR8300 router while Registration to DDNS Service. By specifying username and password, an attacker connected to the router's web interface can execute arbitrary OS commands. The username and password fields are not sanitized correctly and are used as URL construction arguments, allowing URL redirection to an arbitrary server, downloading an arbitrary script file, and eventually executing the file in the device. This issue affects: Linksys MR8300 Router 1.0.	8.2	More Details
CVE-2021-43766	Odyssey passes to server unencrypted bytes from man-in-the-middle When Odyssey is configured to use certificate Common Name for client authentication, a man-in-the-middle attacker can inject arbitrary SQL queries when a connection is first established, despite the use of SSL certificate verification and encryption. This is similar to CVE-2021-23214 for PostgreSQL.	8.1	More Details
CVE-2021-3414	A flaw was found in satellite. When giving granular permission related to the organization, other permissions allowing a user to view and manage other organizations are also granted. The highest threat from this vulnerability is to data confidentiality.	8.1	More Details
CVE-2022-34838	Storing Passwords in a Recoverable Format vulnerability in ABB Zenon 8.20 allows an attacker who successfully exploit the vulnerability may add or alter data points and corresponding attributes. Once such engineering data is used the data visualization will be altered for the end user.	8.1	More Details
CVE-2022-32745	A flaw was found in Samba. Samba AD users can cause the server to access uninitialized data with an LDAP add or modify the request, usually resulting in a segmentation fault.	8.1	More Details
CVE-2022-36120	An issue was discovered in Blue Prism Enterprise 6.0 through 7.01. In a misconfigured environment that exposes the Blue Prism Application server, it is possible for an authenticated user to reverse engineer the Blue Prism software and circumvent access controls for the getChartData administrative function. Using a low/no privilege Blue Prism user account, the attacker can alter the server's settings by abusing the getChartData method, allowing the Blue Prism server to execute any MSSQL stored procedure by name.	8.1	More Details
CVE-2022-29850	Various Lexmark products through 2022-04-27 allow an attacker who has already compromised an affected Lexmark device to maintain persistence across reboots.	8.1	More Details
CVE-2022-25921	All versions of package morgan-json are vulnerable to Arbitrary Code Execution due to missing sanitization of input passed to the Function constructor.	8.1	More Details

CVE Number	Description	Base Score	Reference
CVE-2021-40285	htmly v2.8.1 was discovered to contain an arbitrary file deletion vulnerability via the component \views\backup.html.php.	8.1	More Details
CVE-2021-4125	It was found that the original fix for log4j CVE-2021-44228 and CVE-2021-45046 in the OpenShift metering hive containers was incomplete, as not all JndiLookup.class files were removed. This CVE only applies to the OpenShift Metering hive container images, shipped in OpenShift 4.8, 4.7 and 4.6.	8.1	More Details
CVE-2022-35962	Zulip is an open source team chat and Zulip Mobile is an app for iOS and Andriod users. In Zulip Mobile through version 27.189, a crafted link in a message sent by an authenticated user could lead to credential disclosure if a user follows the link. A patch was released in version 27.190.	8.0	More Details
CVE-2022-2997	Session Fixation in GitHub repository snipe/snipe-it prior to 6.0.10.	8.0	More Details
CVE-2022-36510	H3C GR2200 MiniGR1A0V100R014 was discovered to contain a command injection vulnerability via the param parameter at DelL2tpLNSList.	7.8	More Details
CVE-2022-37079	TOTOLINK A7000R V9.1.0u.6115_B20201022 was discovered to contain a command injection vulnerability via the hostName parameter in the function setOpModeCfg.	7.8	More Details
CVE-2022-37817	Tenda AX1803 v1.0.0.1 was discovered to contain a stack overflow via the function fromSetIpMacBind.	7.8	More Details
CVE-2022-36615	TOTOLINK A3000RU V4.1.2cu.5185_B20201128 was discovered to contain a hardcoded password for root at /etc/shadow.sample.	7.8	More Details
CVE-2022-36614	TOTOLINK A860R V4.1.2cu.5182_B20201027 was discovered to contain a hardcoded password for root at /etc/shadow.sample.	7.8	More Details
CVE-2022-37084	TOTOLINK A7000R V9.1.0u.6115_B20201022 was discovered to contain a stack overflow via the sPort parameter at the addEffect function.	7.8	More Details
CVE-2022-37083	TOTOLINK A7000R V9.1.0u.6115_B20201022 was discovered to contain a command injection vulnerability via the ip parameter at the function setDiagnosisCfg.	7.8	More Details

CVE Number	Description	Base Score	Reference
CVE-2022-36506	H3C Magic NX18 Plus NX18PV100R003 was discovered to contain a stack overflow via the function SetMacAccessMode.	7.8	More Details
CVE-2022-37082	TOTOLINK A7000R V9.1.0u.6115_B20201022 was discovered to contain a command injection vulnerability via the host_time parameter at the function NTPSyncWithHost.	7.8	More Details
CVE-2022-37081	TOTOLINK A7000R V9.1.0u.6115_B20201022 was discovered to contain a command injection vulnerability via the command parameter at setting/setTracerouteCfg.	7.8	More Details
CVE-2022-37080	TOTOLINK A7000R V9.1.0u.6115_B20201022 was discovered to contain a stack overflow via the command parameter at setting/setTracerouteCfg.	7.8	More Details
CVE-2022-37078	TOTOLINK A7000R V9.1.0u.6115_B20201022 was discovered to contain a command injection vulnerability via the lang parameter at /setting/setLanguageCfg.	7.8	More Details
CVE-2022-36509	H3C GR3200 MiniGR1B0V100R014 was discovered to contain a command injection vulnerability via the param parameter at DelL2tpLNSList.	7.8	More Details
CVE-2022-37077	TOTOLINK A7000R V9.1.0u.6115_B20201022 was discovered to contain a stack overflow via the pppoeUser parameter.	7.8	More Details
CVE-2022-36455	TOTOLink A3600R V4.1.2cu.5182_B20201102 was discovered to contain a command injection vulnerability via the username parameter in /cstecgi.cgi.	7.8	More Details
CVE-2022-36612	TOTOLINK A950RG V4.1.2cu.5204_B20210112 was discovered to contain a hardcoded password for root at /etc/shadow.sample.	7.8	More Details
CVE-2022-36507	H3C Magic NX18 Plus NX18PV100R003 was discovered to contain a stack overflow via the function AddWlanMacList.	7.8	More Details
CVE-2022-37819	Tenda AX1803 v1.0.0.1 was discovered to contain a stack overflow via the timezone parameter in the function fromSetSysTime.	7.8	More Details
CVE-2022-36508	H3C Magic NX18 Plus NX18PV100R003 was discovered to contain a stack overflow via the function SetAPInfoById.	7.8	More Details

CVE Number	Description	Base Score	Reference
CVE-2022-37076	TOTOLINK A7000R V9.1.0u.6115_B20201022 was discovered to contain a command injection vulnerability via the FileName parameter in the function UploadFirmwareFile.	7.8	More Details
CVE-2022-37075	TOTOLink A7000R V9.1.0u.6115_B20201022 was discovered to contain a stack overflow via the ip parameter in the function setDiagnosisCfg.	7.8	More Details
CVE-2022-37074	H3C GR-1200W MiniGRW1A0V100R006 was discovered to contain a stack overflow via the function switch_debug_info_set.	7.8	More Details
CVE-2022-37818	Tenda AX1803 v1.0.0.1 was discovered to contain a stack overflow via the list parameter at the function formSetQosBand.	7.8	More Details
CVE-2022-37824	Tenda AX1803 v1.0.0.1 was discovered to contain a stack overflow via the shareSpeed parameter in the function fromSetWifiGusetBasic.	7.8	More Details
CVE-2022-37820	Tenda AX1803 v1.0.0.1 was discovered to contain a stack overflow via the ddnsEn parameter in the function formSetSysToolDDNS.	7.8	More Details
CVE-2020-27800	A heap-based buffer over-read was discovered in the get_le32 function in bele.h in UPX 4.0.0 via a crafted Mach-O file.	7.8	More Details
CVE-2022-36504	H3C Magic NX18 Plus NX18PV100R003 was discovered to contain a stack overflow via the function Edit_BasicSSID.	7.8	More Details
CVE-2022-36611	TOTOLINK A800R V4.1.2cu.5137_B20200730 was discovered to contain a hardcoded password for root at /etc/shadow.sample.	7.8	More Details
CVE-2022-0135	An out-of-bounds write issue was found in the VirGL virtual OpenGL renderer (virglrenderer). This flaw allows a malicious guest to create a specially crafted virgil resource and then issue a VIRTGPU_EXECBUFFER ioctl, leading to a denial of service or possible code execution.	7.8	More Details
CVE-2021-41785	Foxit PDF Reader before 11.1 and PDF Editor before 11.1, and PhantomPDF before 10.1.6, allow attackers to trigger a use-after-free and execute arbitrary code because JavaScript is mishandled.	7.8	More Details

CVE Number	Description	Base Score	Reference
CVE-2020-27796	A heap-based buffer over-read was discovered in the invert_pt_dynamic function in p_lx_elf.cpp in UPX 4.0.0 via a crafted Mach-O file.	7.8	More Details
CVE-2021-41784	Foxit PDF Reader before 11.1 and PDF Editor before 11.1, and PhantomPDF before 10.1.6, allow attackers to trigger a use-after-free and execute arbitrary code because JavaScript is mishandled.	7.8	More Details
CVE-2022-0358	A flaw was found in the QEMU virtio-fs shared file system daemon (virtiofsd) implementation. This flaw is strictly related to CVE-2018-13405. A local guest user can create files in the directories shared by virtio-fs with unintended group ownership in a scenario where a directory is SGID to a certain group and is writable by a user who is not a member of the group. This could allow a malicious unprivileged user inside the guest to gain access to resources accessible to the root group, potentially escalating their privileges within the guest. A malicious local user in the host might also leverage this unexpected executable file created by the guest to escalate their privileges on the host system.	7.8	More Details
CVE-2022-0367	A heap-based buffer overflow flaw was found in libmodbus in function modbus_reply() in src/modbus.c.	7.8	More Details
CVE-2021-41783	Foxit PDF Reader before 11.1 and PDF Editor before 11.1, and PhantomPDF before 10.1.6, allow attackers to trigger a use-after-free and execute arbitrary code because JavaScript is mishandled.	7.8	More Details
CVE-2020-27799	A heap-based buffer over-read was discovered in the acc_ua_get_be32 function in miniacc.h in UPX 4.0.0 via a crafted Mach-O file.	7.8	More Details
CVE-2020-27801	A heap-based buffer over-read was discovered in the get_le64 function in bele.h in UPX 4.0.0 via a crafted Mach-O file.	7.8	More Details
CVE-2022-37821	Tenda AX1803 v1.0.0.1 was discovered to contain a stack overflow via the ProvinceCode parameter in the function formSetProvince.	7.8	More Details
CVE-2021-41782	Foxit PDF Reader before 11.1 and PDF Editor before 11.1, and PhantomPDF before 10.1.6, allow attackers to trigger a use-after-free and execute arbitrary code because JavaScript is mishandled.	7.8	More Details
CVE-2022-36610	TOTOLINK A720R V4.1.5cu.532_B20210610 was discovered to contain a hardcoded password for root at /etc/shadow.sample.	7.8	More Details

CVE Number	Description	Base Score	Reference
CVE-2021-41781	Foxit PDF Reader before 11.1 and PDF Editor before 11.1, and PhantomPDF before 10.1.6, allow attackers to trigger a use-after-free and execute arbitrary code because JavaScript is mishandled.	7.8	More Details
CVE-2021-41780	Foxit PDF Reader before 11.1 and PDF Editor before 11.1, and PhantomPDF before 10.1.6, allow attackers to trigger a use-after-free and execute arbitrary code because JavaScript is mishandled.	7.8	More Details
CVE-2022-38511	TOTOLINK A810R V5.9c.4050_B20190424 was discovered to contain a command injection vulnerability via the component downloadFile.cgi.	7.8	More Details
CVE-2022-38510	Tenda_TX9pro V22.03.02.10 was discovered to contain a buffer overflow via the component httpd/SetNetControlList.	7.8	More Details
CVE-2022-36616	TOTOLINK A810R V4.1.2cu.5182_B20201026 and V5.9c.4050_B20190424 was discovered to contain a hardcoded password for root at /etc/shadow.sample.	7.8	More Details
CVE-2022-2982	Use After Free in GitHub repository vim/vim prior to 9.0.0260.	7.8	More Details
CVE-2022-37823	Tenda AX1803 v1.0.0.1 was discovered to contain a stack overflow via the list parameter in the function formSetVirtualSer.	7.8	More Details
CVE-2022-37822	Tenda AX1803 v1.0.0.1 was discovered to contain a stack overflow via the function fromSetRouteStatic.	7.8	More Details
CVE-2022-36505	H3C Magic NX18 Plus NX18PV100R003 was discovered to contain a stack overflow via the function EDitusergroup.	7.8	More Details
CVE-2022-36493	H3C Magic NX18 Plus NX18PV100R003 was discovered to contain a stack overflow via the function SetAPWifiorLedInfoById.	7.8	More Details
CVE-2022-36503	H3C Magic NX18 Plus NX18PV100R003 was discovered to contain a stack overflow via the function UpdateMacClone.	7.8	More Details
CVE-2022-36460	TOTOLINK A3700R V9.1.2u.6134_B20201202 was discovered to contain a command injection vulnerability via the FileName parameter in the function UploadFirmwareFile.	7.8	More Details

CVE Number	Description	Base Score	Reference
CVE-2022-32840	This issue was addressed with improved checks. This issue is fixed in macOS Monterey 12.5, watchOS 8.7, iOS 15.6 and iPadOS 15.6. An app may be able to execute arbitrary code with kernel privileges.	7.8	More Details
CVE-2022-32894	An out-of-bounds write issue was addressed with improved bounds checking. This issue is fixed in iOS 15.6.1 and iPadOS 15.6.1, macOS Monterey 12.5.1. An application may be able to execute arbitrary code with kernel privileges. Apple is aware of a report that this issue may have been actively exploited.	7.8	More Details
CVE-2022-30984	A buffer overflow vulnerability in the Rubrik Backup Service (RBS) Agent for Linux or Unix-based systems in Rubrik CDM 7.0.1, 7.0.1-p1, 7.0.1-p2 or 7.0.1-p3 before CDM 7.0.2-p2 could allow a local attacker to obtain root privileges by sending a crafted message to the RBS agent.	7.8	More Details
CVE-2022-36456	TOTOLink A720R V4.1.5cu.532_B20210610 was discovered to contain a command injection vulnerability via the username parameter in /cstecgi.cgi.	7.8	More Details
CVE-2022-36458	TOTOLINK A3700R V9.1.2u.6134_B20201202 was discovered to contain a command injection vulnerability via the command parameter in the function setTracerouteCfg.	7.8	More Details
CVE-2022-36459	TOTOLINK A3700R V9.1.2u.6134_B20201202 was discovered to contain a command injection vulnerability via the host_time parameter in the function NTPSyncWithHost.	7.8	More Details
CVE-2022-36461	TOTOLINK A3700R V9.1.2u.6134_B20201202 was discovered to contain a command injection vulnerability via the hostName parameter in the function setOpModeCfg.	7.8	More Details
CVE-2022-32813	The issue was addressed with improved memory handling. This issue is fixed in macOS Monterey 12.5, macOS Big Sur 11.6.8, Security Update 2022-005 Catalina, iOS 15.6 and iPadOS 15.6, tvOS 15.6, watchOS 8.7. An app with root privileges may be able to execute arbitrary code with kernel privileges.	7.8	More Details
CVE-2022-36502	H3C Magic NX18 Plus NX18PV100R003 was discovered to contain a stack overflow via the function UpdateWanParams.	7.8	More Details
CVE-2022-36463	TOTOLINK A3700R V9.1.2u.6134_B20201202 was discovered to contain a stack overflow via the command parameter in the function setTracerouteCfg.	7.8	More Details

CVE Number	Description	Base Score	Reference
CVE-2022-36464	TOTOLINK A3700R V9.1.2u.6134_B20201202 was discovered to contain a stack overflow via the sPort parameter in the function setIpPortFilterRules.	7.8	More Details
CVE-2022-36465	TOTOLINK A3700R V9.1.2u.6134_B20201202 was discovered to contain a stack overflow via the pppoeUser parameter.	7.8	More Details
CVE-2022-36466	TOTOLINK A3700R V9.1.2u.6134_B20201202 was discovered to contain a stack overflow via the ip parameter in the function setDiagnosisCfg.	7.8	More Details
CVE-2022-36467	H3C B5 Mini B5MiniV100R005 was discovered to contain a stack overflow via the function EditMacList.d.	7.8	More Details
CVE-2022-32837	This issue was addressed with improved checks. This issue is fixed in macOS Monterey 12.5, tvOS 15.6, iOS 15.6 and iPadOS 15.6. An app may be able to cause unexpected system termination or write kernel memory.	7.8	More Details
CVE-2022-32812	The issue was addressed with improved memory handling. This issue is fixed in macOS Monterey 12.5, macOS Big Sur 11.6.8, Security Update 2022-005 Catalina. An app may be able to execute arbitrary code with kernel privileges.	7.8	More Details
CVE-2022-36469	H3C B5 Mini B5MiniV100R005 was discovered to contain a stack overflow via the function SetAPWifiorLedInfoById.	7.8	More Details
CVE-2021-4041	A flaw was found in ansible-runner. An improper escaping of the shell command, while calling the ansible_runner.interface.run_command, can lead to parameters getting executed as host's shell command. A developer could unintentionally write code that gets executed in the host rather than the virtual environment.	7.8	More Details
CVE-2022-3037	Use After Free in GitHub repository vim/vim prior to 9.0.0322.	7.8	More Details
CVE-2022-37173	An issue in the installer of gvim 9.0.0000 allows authenticated attackers to execute arbitrary code via a binary hijacking attack on C:\Program.exe.	7.8	More Details
CVE-2022-37172	Incorrect access control in the install directory (C:\msys64) of Msys2 v20220603 and below allows authenticated attackers to execute arbitrary code via overwriting binaries located in the directory.	7.8	More Details

CVE Number	Description	Base Score	Reference
CVE-2021-3999	A flaw was found in glibc. An off-by-one buffer overflow and underflow in getcwd() may lead to memory corruption when the size of the buffer is exactly 1. A local attacker who can control the input buffer and size passed to getcwd() in a setuid program could use this flaw to potentially execute arbitrary code and escalate their privileges on the system.	7.8	More Details
CVE-2021-4028	A flaw in the Linux kernel's implementation of RDMA communications manager listener code allowed an attacker with local access to setup a socket to listen on a high port allowing for a list element to be used after free. Given the ability to execute code, a local attacker could leverage this use-after-free to crash the system or possibly escalate privileges on the system.	7.8	More Details
CVE-2021-4037	A vulnerability was found in the fs/inode.c:inode_init_owner() function logic of the LInux kernel that allows local users to create files for the XFS file-system with an unintended group ownership and with group execution and SGID permission bits set, in a scenario where a directory is SGID and belongs to a certain group and is writable by a user who is not a member of this group. This can lead to excessive permissions granted in case when they should not. This vulnerability is similar to the previous CVE-2018-13405 and adds the missed fix for the XFS.	7.8	More Details
CVE-2022-3016	Use After Free in GitHub repository vim/vim prior to 9.0.0286.	7.8	More Details
CVE-2022-32811	A memory corruption vulnerability was addressed with improved locking. This issue is fixed in macOS Monterey 12.5, macOS Big Sur 11.6.8, Security Update 2022-005 Catalina. An app may be able to execute arbitrary code with kernel privileges.	7.8	More Details
CVE-2021-20260	A flaw was found in the Foreman project. The Datacenter plugin exposes the password through the API to an authenticated local attacker with view_hosts permission. The highest threat from this vulnerability is to data confidentiality and integrity as well as system availability.	7.8	More Details
CVE-2022-24107	Xpdf prior to 4.04 lacked an integer overflow check in JPXStream.cc.	7.8	More Details
CVE-2022-24106	In Xpdf prior to 4.04, the DCT (JPEG) decoder was incorrectly allowing the 'interleaved' flag to be changed after the first scan of the image, leading to an unknown integer-related vulnerability in Stream.cc.	7.8	More Details

CVE Number	Description	Base Score	Reference
CVE-2022-2978	A flaw use after free in the Linux kernel NILFS file system was found in the way user triggers function security_inode_alloc to fail with following call to function nilfs_mdt_destroy. A local user could use this flaw to crash the system or potentially escalate their privileges on the system.	7.8	More Details
CVE-2022-38784	Poppler prior to and including 22.08.0 contains an integer overflow in the JBIG2 decoder (JBIG2Stream::readTextRegionSeg() in JBIGStream.cc). Processing a specially crafted PDF file or JBIG2 image could lead to a crash or the execution of arbitrary code. This is similar to the vulnerability described by CVE-2022-38171 in Xpdf.	7.8	More Details
CVE-2022-32810	The issue was addressed with improved memory handling. This issue is fixed in macOS Monterey 12.5, watchOS 8.7, iOS 15.6 and iPadOS 15.6. An app may be able to execute arbitrary code with kernel privileges.	7.8	More Details
CVE-2022-36468	H3C B5 Mini B5MiniV100R005 was discovered to contain a stack overflow via the function Asp_SetTimingtimeWifiAndLed.	7.8	More Details
CVE-2022-36462	TOTOLINK A3700R V9.1.2u.6134_B20201202 was discovered to contain a stack overflow via the lang parameter in the function setLanguageCfg.	7.8	More Details
CVE-2022-36613	TOTOLINK N600R V4.3.0cu.7647_B20210106 was discovered to contain a hardcoded password for root at /etc/shadow.sample.	7.8	More Details
CVE-2022-36482	TOTOLINK N350RT V9.3.5u.6139_B20201216 was discovered to contain a command injection vulnerability via the lang parameter in the function setLanguageCfg.	7.8	More Details
CVE-2022-36492	H3C Magic NX18 Plus NX18PV100R003 was discovered to contain a stack overflow via the function AddMacList.	7.8	More Details
CVE-2022-36495	H3C Magic NX18 Plus NX18PV100R003 was discovered to contain a stack overflow via the function addactionlist.	7.8	More Details
CVE-2022-36496	H3C Magic NX18 Plus NX18PV100R003 was discovered to contain a stack overflow via the function SetMobileAPInfoById.	7.8	More Details
CVE-2022-36497	H3C Magic NX18 Plus NX18PV100R003 was discovered to contain a stack overflow via the function Edit_BasicSSID_5G.	7.8	More Details

CVE Number	Description	Base Score	Reference
CVE-2022-36498	H3C Magic NX18 Plus NX18PV100R003 was discovered to contain a stack overflow via the function Asp_SetTimingtimeWifiAndLed.	7.8	More Details
CVE-2022-36491	H3C Magic NX18 Plus NX18PV100R003 was discovered to contain a stack overflow via the function UpdateIpv6Params.	7.8	More Details
CVE-2022-36490	H3C Magic NX18 Plus NX18PV100R003 was discovered to contain a stack overflow via the function EditMacList.	7.8	More Details
CVE-2022-36489	H3C Magic NX18 Plus NX18PV100R003 was discovered to contain a stack overflow via the function EnableIpv6.	7.8	More Details
CVE-2022-36488	TOTOLINK N350RT V9.3.5u.6139_B20201216 was discovered to contain a stack overflow via the sPort parameter in the function setIpPortFilterRules.	7.8	More Details
CVE-2022-36499	H3C Magic NX18 Plus NX18PV100R003 was discovered to contain a stack overflow via the function DEleteusergroup.	7.8	More Details
CVE-2022-36487	TOTOLINK N350RT V9.3.5u.6139_B20201216 was discovered to contain a command injection vulnerability via the command parameter in the function setTracerouteCfg.	7.8	More Details
CVE-2022-36486	TOTOLINK N350RT V9.3.5u.6139_B20201216 was discovered to contain a command injection vulnerability via the FileName parameter in the function UploadFirmwareFile.	7.8	More Details
CVE-2022-36485	TOTOLINK N350RT V9.3.5u.6139_B20201216 was discovered to contain a command injection vulnerability via the hostName parameter in the function setOpModeCfg.	7.8	More Details
CVE-2022-36483	TOTOLINK N350RT V9.3.5u.6139_B20201216 was discovered to contain a stack overflow via the pppoeUser parameter.	7.8	More Details
CVE-2022-36484	TOTOLINK N350RT V9.3.5u.6139_B20201216 was discovered to contain a stack overflow via the function setDiagnosisCfg.	7.8	More Details
CVE-2022-36500	H3C Magic NX18 Plus NX18PV100R003 was discovered to contain a stack overflow via the function EditWlanMacList.	7.8	More Details

CVE Number	Description	Base Score	Reference
CVE-2022-36479	TOTOLINK N350RT V9.3.5u.6139_B20201216 was discovered to contain a command injection vulnerability via the host_time parameter in the function NTPSyncWithHost.	7.8	More Details
CVE-2022-36470	H3C B5 Mini B5MiniV100R005 was discovered to contain a stack overflow via the function SetAP5GWifiById.	7.8	More Details
CVE-2022-36471	H3C B5 Mini B5MiniV100R005 was discovered to contain a stack overflow via the function SetMacAccessMode.	7.8	More Details
CVE-2022-36472	H3C B5 Mini B5MiniV100R005 was discovered to contain a stack overflow via the function SetMobileAPInfoById.	7.8	More Details
CVE-2022-36473	H3C B5 Mini B5MiniV100R005 was discovered to contain a stack overflow via the function Edit_BasicSSID_5G.	7.8	More Details
CVE-2022-36474	H3C B5 Mini B5MiniV100R005 was discovered to contain a stack overflow via the function WlanWpsSet.	7.8	More Details
CVE-2022-36475	H3C B5 Mini B5MiniV100R005 was discovered to contain a stack overflow via the function AddMacList.	7.8	More Details
CVE-2022-36477	H3C B5 Mini B5MiniV100R005 was discovered to contain a stack overflow via the function AddWlanMacList.	7.8	More Details
CVE-2022-36501	H3C Magic NX18 Plus NX18PV100R003 was discovered to contain a stack overflow via the function UpdateSnat.	7.8	More Details
CVE-2022-36478	H3C B5 Mini B5MiniV100R005 was discovered to contain a stack overflow via the function Edit_BasicSSID.	7.8	More Details
CVE-2022-36480	TOTOLINK N350RT V9.3.5u.6139_B20201216 was discovered to contain a stack overflow via the command parameter in the function setTracerouteCfg.	7.8	More Details
CVE-2022-36481	TOTOLINK N350RT V9.3.5u.6139_B20201216 was discovered to contain a command injection vulnerability via the ip parameter in the function setDiagnosisCfg.	7.8	More Details

CVE Number	Description	Base Score	Reference
CVE-2022-36494	H3C Magic NX18 Plus NX18PV100R003 was discovered to contain a stack overflow via the function edditactionlist.	7.8	More Details
CVE-2022-2464	Rockwell Automation ISaGRAF Workbench software versions 6.0 through 6.6.9 are affected by a Path Traversal vulnerability. Crafted malicious files can allow an attacker to traverse the file system when opened by ISaGRAF Workbench. If successfully exploited, an attacker could overwrite existing files and create additional files with the same permissions of the ISaGRAF Workbench software. User interaction is required for this exploit to be successful.	7.7	More Details
CVE-2022-37317	Archer Platform 6.x before 6.11 P3 contain an HTML injection vulnerability. An authenticated remote attacker could potentially exploit this vulnerability by tricking a victim application user to execute malicious code in the context of the web application. 6.10 P4 (6.10.0.4) and 6.11 P2 HF4 (6.11.0.2.4) are also fixed releases.	7.6	More Details
CVE-2021-3703	It was found that the CVE-2021-27918, CVE-2021-31525 and CVE-2021-33196 have been incorrectly mentioned as fixed in RHSA for Serverless 1.16.0 and Serverless client kn 1.16.0. These have been fixed with Serverless 1.17.0.	7.5	More Details
CVE-2021-3859	A flaw was found in Undertow that tripped the client-side invocation timeout with certain calls made over HTTP2. This flaw allows an attacker to carry out denial of service attacks.	7.5	More Details
CVE-2022-36537	ZK Framework v9.6.1, 9.6.0.1, 9.5.1.3, 9.0.1.2 and 8.6.4.1 allows attackers to access sensitive information via a crafted POST request sent to the component AuUploader.	7.5	More Details
CVE-2021-3632	A flaw was found in Keycloak. This vulnerability allows anyone to register a new security device or key when there is not a device already registered for any user by using the WebAuthn password-less login flow.	7.5	More Details
CVE-2022-0217	It was discovered that an internal Prosody library to load XML based on libexpat does not properly restrict the XML features allowed in parsed XML data. Given suitable attacker input, this results in expansion of recursive entity references from DTDs (CWE-776). In addition, depending on the libexpat version used, it may also allow injections using XML External Entity References (CWE-611).	7.5	More Details
CVE-2022-38794	Zaver through 2020-12-15 allows directory traversal via the GET /.. substring.	7.5	More Details

CVE Number	Description	Base Score	Reference
CVE-2022-38571	Tenda M3 V1.0.0.12(4856) was discovered to contain a buffer overflow in the function formSetGuideListItem.	7.5	More Details
CVE-2022-36521	Insecure permissions in cskefu v7.0.1 allows unauthenticated attackers to arbitrarily add administrator accounts.	7.5	More Details
CVE-2022-37151	There is an unauthorized access vulnerability in Online Diagnostic Lab Management System 1.0.	7.5	More Details
CVE-2022-38562	Tenda M3 V1.0.0.12(4856) was discovered to contain a heap buffer overflow vulnerability in the function formSetFixTools. This vulnerability allows attackers to cause a Denial of Service (DoS) via the lan parameter.	7.5	More Details
CVE-2022-38563	Tenda M3 V1.0.0.12(4856) was discovered to contain a heap buffer overflow vulnerability in the function formSetFixTools. This vulnerability allows attackers to cause a Denial of Service (DoS) via the MACAddr parameter.	7.5	More Details
CVE-2022-38564	Tenda M3 V1.0.0.12(4856) was discovered to contain a buffer overflow vulnerability in the function formSetPicListItem. This vulnerability allows attackers to cause a Denial of Service (DoS) via the adItemUID parameter.	7.5	More Details
CVE-2022-38565	Tenda M3 V1.0.0.12(4856) was discovered to contain a heap buffer overflow vulnerability in the function formEmailTest. This vulnerability allows attackers to cause a Denial of Service (DoS) via the mailpwd parameter.	7.5	More Details
CVE-2022-38570	Tenda M3 V1.0.0.12(4856) was discovered to contain a stack overflow in the function formDelPushedAd. This vulnerability allows attackers to cause a Denial of Service (DoS) via the adPushUID parameter.	7.5	More Details
CVE-2022-38567	Tenda M3 V1.0.0.12(4856) was discovered to contain a stack overflow vulnerability in the function formSetAdConfigInfo. This vulnerability allows attackers to cause a Denial of Service (DoS) via the authIPs parameter.	7.5	More Details
CVE-2022-38568	Tenda M3 V1.0.0.12(4856) was discovered to contain a heap buffer overflow vulnerability in the function formSetFixTools. This vulnerability allows attackers to cause a Denial of Service (DoS) via the hostname parameter.	7.5	More Details

CVE Number	Description	Base Score	Reference
CVE-2022-35192	D-Link Wireless AC1200 Dual Band VDSL ADSL Modem Router DSL-3782 Firmware v1.01 allows unauthenticated attackers to cause a Denial of Service (DoS) via the User parameter or Pwd parameter to Login.asp.	7.5	More Details
CVE-2022-38569	Tenda M3 V1.0.0.12(4856) was discovered to contain a stack overflow in the function formDelAd.	7.5	More Details
CVE-2022-24375	The package node-opcua before 2.74.0 are vulnerable to Denial of Service (DoS) when bypassing the limitations for excessive memory consumption by sending multiple CloseSession requests with the deleteSubscription parameter equal to False.	7.5	More Details
CVE-2022-38566	Tenda M3 V1.0.0.12(4856) was discovered to contain a heap buffer overflow vulnerability in the function formEmailTest. This vulnerability allows attackers to cause a Denial of Service (DoS) via the mailname parameter.	7.5	More Details
CVE-2022-0084	A flaw was found in XNIO, specifically in the notifyReadClosed method. The issue revealed this method was logging a message to another expected end. This flaw allows an attacker to send flawed requests to a server, possibly causing log contention-related performance concerns or an unwanted disk fill-up.	7.5	More Details
CVE-2022-37681	Hitachi Kokusai Electric Newtork products for monitoring system (Camera, Decoder and Encoder) and below allows attckers to perform a directory traversal via a crafted GET request to the endpoint /ptippage.cgi. Security information ID hitachi-sec-2022-001 contains fixes for the issue.	7.5	More Details
CVE-2021-3998	A flaw was found in glibc. The realpath() function can mistakenly return an unexpected value, potentially leading to information leakage and disclosure of sensitive data.	7.5	More Details
CVE-2022-37680	An improper authentication for critical function issue in Hitachi Kokusai Electric Network products for monitoring system (Camera, Decoder and Encoder) and bellow allows attckers to remotely reboot the device via a crafted POST request to the endpoint /ptipupgrade.cgi. Security information ID hitachi-sec-2022-001 contains fixes for the issue.	7.5	More Details
CVE-2022-22728	A flaw in Apache libapreq2 versions 2.16 and earlier could cause a buffer overflow while processing multipart form uploads. A remote attacker could send a request causing a process crash which could lead to a denial of service attack.	7.5	More Details

CVE Number	Description	Base Score	Reference
CVE-2022-25857	The package org.yaml:snakeyaml from 0 and before 1.31 are vulnerable to Denial of Service (DoS) due missing to nested depth limitation for collections.	7.5	More Details
CVE-2021-4213	A flaw was found in JSS, where it did not properly free up all memory. Over time, the wasted memory builds up in the server memory, saturating the server's RAM. This flaw allows an attacker to force the invocation of an out-of-memory process, causing a denial of service.	7.5	More Details
CVE-2022-39028	telnetd in GNU Inetutils through 2.3, MIT krb5-appl through 1.0.3, and derivative works has a NULL pointer dereference via 0xff 0xf7 or 0xff 0xf8. In a typical installation, the telnetd application would crash but the telnet service would remain available through inetd. However, if the telnetd application has many crashes within a short time interval, the telnet service would become unavailable after inetd logs a "telnet/tcp server failing (looping), service terminated" error. NOTE: MIT krb5-appl is not supported upstream but is shipped by a few Linux distributions. The affected code was removed from the supported MIT Kerberos 5 (aka krb5) product many years ago, at version 1.8.	7.5	More Details
CVE-2022-36034	nitrado.js is a type safe wrapper for the Nitrado API. Possible ReDoS with lib input of `{{` and with many repetitions of `{{l`. This issue has been patched in all versions above `0.2.5`. There are currently no known workarounds.	7.5	More Details
CVE-2022-36200	In FiberHome VDSL2 Modem HG150-Ub_V3.0, Credentials of Admin are submitted in URL, which can be logged/sniffed.	7.5	More Details
CVE-2022-36552	Tenda AC6(AC1200) v5.0 Firmware v02.03.01.114 and below contains an issue in the component /cgi-bin/DownloadFlash which allows attackers to steal all data such as source code and system files via a crafted GET request.	7.5	More Details
CVE-2022-1199	A flaw was found in the Linux kernel. This flaw allows an attacker to crash the Linux kernel by simulating amateur radio from the user space, resulting in a null-ptr-deref vulnerability and a use-after-free vulnerability.	7.5	More Details
CVE-2022-0934	A single-byte, non-arbitrary write/use-after-free flaw was found in dnsmasq. This flaw allows an attacker who sends a crafted packet processed by dnsmasq, potentially causing a denial of service.	7.5	More Details
CVE-2022-32793	Multiple out-of-bounds write issues were addressed with improved bounds checking. This issue is fixed in macOS Monterey 12.5, watchOS 8.7, tvOS 15.6, iOS 15.6 and iPadOS 15.6. An app may be able to disclose kernel memory.	7.5	More Details

CVE Number	Description	Base Score	Reference
CVE-2022-37237	An attacker can send malicious RTMP requests to make the ZLMediaKit server crash remotely. Affected version is below commit 7d8b212a3c3368bc2f6507cb74664fc419eb9327.	7.5	More Details
CVE-2021-0947	The method PVRSRVBridgeTLDiscoverStreams allocates puiStreamsInt on the heap, fills the contents of the buffer via TLServerDiscoverStreamsKM, and then copies the buffer to userspace. The method TLServerDiscoverStreamsKM may fail for several reasons including invalid sizes. If this method fails the buffer will be left uninitialized and despite the error will still be copied to userspace. Kernel leak of uninitialized heap data with no privs required.Product: AndroidVersions: Android SoCAndroid ID: A-236838960	7.5	More Details
CVE-2021-0946	The method PVRSRVBridgePMRPDumpSymbolicAddr allocates puiMemspaceNameInt on the heap, fills the contents of the buffer via PMR_PDumpSymbolicAddr, and then copies the buffer to userspace. The method PMR_PDumpSymbolicAddr may fail, and if it does the buffer will be left uninitialized and despite the error will still be copied to userspace. Kernel leak of uninitialized heap data with no privs required.Product: AndroidVersions: Android SoCAndroid ID: A-236846966	7.5	More Details
CVE-2021-42521	There is a NULL pointer dereference vulnerability in VTK before 9.2.5, and it lies in IO/Infovis/vtkXMLTreeReader.cxx. The vendor didn't check the return value of libxml2 API 'xmlDocGetRootElement', and try to dereference it. It is unsafe as the return value can be NULL and that NULL pointer dereference may crash the application.	7.5	More Details
CVE-2021-42522	There is a Information Disclosure vulnerability in anjuta/plugins/document-manager/anjuta-bookmarks.c. This issue was caused by the incorrect use of libxml2 API. The vendor forgot to call 'g_free()' to release the return value of 'xmlGetProp()'.	7.5	More Details
CVE-2021-42523	There are two Information Disclosure vulnerabilities in colord, and they lie in colord/src/cd-device-db.c and colord/src/cd-profile-db.c separately. They exist because the 'err_msg' of 'sqlite3_exec' is not releasing after use, while libxml2 emphasizes that the caller needs to release it.	7.5	More Details
CVE-2022-0400	An out-of-bounds read vulnerability was discovered in linux kernel in the smc protocol stack, causing remote dos.	7.5	More Details
CVE-2021-0891	An unprivileged app can trigger PowerVR driver to return an uninitialized heap memory causing information disclosure.Product: AndroidVersions: Android SoCAndroid ID: A-236849490	7.5	More Details

CVE Number	Description	Base Score	Reference
CVE-2022-2255	A vulnerability was found in mod_wsgi. The X-Client-IP header is not removed from a request from an untrusted proxy, allowing an attacker to pass the X-Client-IP header to the target WSGI application because the condition to remove it is missing.	7.5	More Details
CVE-2022-27812	Flooding SNS firewall versions 3.7.0 to 3.7.29, 3.11.0 to 3.11.17, 4.2.0 to 4.2.10, and 4.3.0 to 4.3.6 with specific forged traffic, can lead to SNS DoS.	7.5	More Details
CVE-2022-27563	An unauthenticated user can overload a part of HCL VersionVault Express and cause a denial of service.	7.5	More Details
CVE-2022-25903	The package opcua from 0.0.0 are vulnerable to Denial of Service (DoS) via the ExtensionObjects and Variants objects, when it allows unlimited nesting levels, which could result in a stack overflow even if the message size is less than the maximum allowed.	7.5	More Details
CVE-2022-37177	HireVue Hiring Platform V1.0 suffers from Use of a Broken or Risky Cryptographic Algorithm. NOTE: this is disputed by the vendor for multiple reasons, e.g., it is inconsistent with CVE ID assignment rules for cloud services, and no product with version V1.0 exists. Furthermore, the rail-fence cipher has been removed, and TLS 1.2 is now used for encryption.	7.5	More Details
CVE-2021-3563	A flaw was found in openstack-keystone. Only the first 72 characters of an application secret are verified allowing attackers bypass some password complexity which administrators may be counting on. The highest threat from this vulnerability is to data confidentiality and integrity.	7.4	More Details
CVE-2022-36226	SiteServerCMS 5.X has a Remote-download-Getshell-vulnerability via /SiteServer/Ajax/ajaxOtherService.aspx.	7.2	More Details
CVE-2022-2261	The WPIDE WordPress plugin before 3.0 does not sanitize and validate the filename parameter before using it in a require statement in the admin dashboard, leading to a Local File Inclusion issue.	7.2	More Details
CVE-2020-26938	In oauth2-server (aka node-oauth2-server) through 3.1.1, the value of the redirect_uri parameter received during the authorization and token request is checked against an incorrect URI pattern ("[a-zA-Z][a-zA-Z0-9+.-]+:") before making a redirection. This allows a malicious client to pass an XSS payload through the redirect_uri parameter while making an authorization request. NOTE: this vulnerability is similar to CVE-2020-7741.	7.2	More Details

CVE Number	Description	Base Score	Reference
CVE-2022-2559	The Fluent Support WordPress plugin before 1.5.8 does not properly sanitise, validate and escape various parameters before using them in an SQL statement, leading to an SQL Injection vulnerability exploitable by high privilege users	7.2	More Details
CVE-2022-1123	The Leaflet Maps Marker (Google Maps, OpenStreetMap, Bing Maps) WordPress plugin before 3.12.5 does not properly sanitize some parameters before inserting them into SQL queries. As a result, high privilege users could perform SQL injection attacks.	7.2	More Details
CVE-2021-4204	An out-of-bounds (OOB) memory access flaw was found in the Linux kernel's eBPF due to an Improper Input Validation. This flaw allows a local attacker with a special privilege to crash the system or leak internal information.	7.1	More Details
CVE-2022-0284	A heap-based-buffer-over-read flaw was found in ImageMagick's GetPixelAlpha() function of 'pixel-accessor.h'. This vulnerability is triggered when an attacker passes a specially crafted Tagged Image File Format (TIFF) image to convert it into a PICON file format. This issue can potentially lead to a denial of service and information disclosure.	7.1	More Details
CVE-2022-0497	A vulnerbiility was found in Openscad, where a .scad file with no trailing newline could cause an out-of-bounds read during parsing of annotations.	7.1	More Details
CVE-2022-0850	A vulnerability was found in linux kernel, where an information leak occurs via ext4_extent_header to userspace.	7.1	More Details
CVE-2022-36115	An issue was discovered in Blue Prism Enterprise 6.0 through 7.01. In a misconfigured environment that exposes the Blue Prism Application server, it is possible for an authenticated user to reverse engineer the Blue Prism software and circumvent access controls for unintended functionality. An attacker can abuse the CreateProcessAutosave() method to inject their own functionality into a development process. If (upon a warning) a user decides to recover unsaved work by using the last saved version, the malicious code could enter the workflow. Should the process action stages not be fully reviewed before publishing, this could result in the malicious code being run in a production environment.	7.1	More Details
CVE-2022-2961	A use-after-free flaw was found in the Linux kernel’s PLP Rose functionality in the way a user triggers a race condition by calling bind while simultaneously triggering the rose_bind() function. This flaw allows a local user to crash or potentially escalate their privileges on the system.	7.0	More Details

CVE Number	Description	Base Score	Reference
CVE-2021-3864	A flaw was found in the way the dumpable flag setting was handled when certain SUID binaries executed its descendants. The prerequisite is a SUID binary that sets real UID equal to effective UID, and real GID equal to effective GID. The descendant will then have a dumpable value set to 1. As a result, if the descendant process crashes and core_pattern is set to a relative value, its core dump is stored in the current directory with uid:gid permissions. An unprivileged local user with eligible root SUID binary could use this flaw to place core dumps into root-owned directories, potentially resulting in escalation of privileges.	7.0	More Details
CVE-2022-2959	A race condition was found in the Linux kernel's watch queue due to a missing lock in pipe_resize_ring(). The specific flaw exists within the handling of pipe buffers. The issue results from the lack of proper locking when performing operations on an object. This flaw allows a local user to crash the system or escalate their privileges on the system.	7.0	More Details
CVE-2022-37318	Archer Platform 6.9 SP2 P2 before 6.11 P3 (6.11.0.3) contain a reflected XSS vulnerability. A remote unauthenticated malicious Archer user could potentially exploit this vulnerability by tricking a victim application user into supplying malicious JavaScript code to the vulnerable web application. This code is then reflected to the victim and gets executed by the web browser in the context of the vulnerable web application. 6.10 P4 (6.10.0.4) and 6.11 P2 HF4 (6.11.0.2.4) are also fixed releases.	7.0	More Details
CVE-2022-2991	A heap-based buffer overflow was found in the Linux kernel's LightNVM subsystem. The issue results from the lack of proper validation of the length of user-supplied data prior to copying it to a fixed-length heap-based buffer. This vulnerability allows a local attacker to escalate privileges and execute arbitrary code in the context of the kernel. The attacker must first obtain the ability to execute high-privileged code on the target system to exploit this vulnerability.	6.7	More Details
CVE-2022-34301	A flaw was found in CryptoPro Secure Disk bootloaders before 2022-06-01. An attacker may use this bootloader to bypass or tamper with Secure Boot protections. In order to load and execute arbitrary code in the pre-boot stage, an attacker simply needs to replace the existing signed bootloader currently in use with this bootloader. Access to the EFI System Partition is required for booting using external media.	6.7	More Details
CVE-2022-34302	A flaw was found in New Horizon Datasys bootloaders before 2022-06-01. An attacker may use this bootloader to bypass or tamper with Secure Boot protections. In order to load and execute arbitrary code in the pre-boot stage, an attacker simply needs to replace the existing signed bootloader currently in use with this bootloader. Access to the EFI System Partition is required for booting using external media.	6.7	More Details

CVE Number	Description	Base Score	Reference
CVE-2022-34303	A flaw was found in Eurosoft bootloaders before 2022-06-01. An attacker may use this bootloader to bypass or tamper with Secure Boot protections. In order to load and execute arbitrary code in the pre-boot stage, an attacker simply needs to replace the existing signed bootloader currently in use with this bootloader. Access to the EFI System Partition is required for booting using external media.	6.7	More Details
CVE-2021-35938	A symbolic link issue was found in rpm. It occurs when rpm sets the desired permissions and credentials after installing a file. A local unprivileged user could use this flaw to exchange the original file with a symbolic link to a security-critical file and escalate their privileges on the system. The highest threat from this vulnerability is to data confidentiality and integrity as well as system availability.	6.7	More Details
CVE-2021-35939	It was found that the fix for CVE-2017-7500 and CVE-2017-7501 was incomplete: the check was only implemented for the parent directory of the file to be created. A local unprivileged user who owns another ancestor directory could potentially use this flaw to gain root privileges. The highest threat from this vulnerability is to data confidentiality and integrity as well as system availability.	6.7	More Details
CVE-2021-4178	A arbitrary code execution flaw was found in the Fabric 8 Kubernetes client affecting versions 5.0.0-beta-1 and above. Due to an improperly configured YAML parsing, this will allow a local and privileged attacker to supply malicious YAML.	6.7	More Details
CVE-2022-20865	A vulnerability in the CLI of Cisco FXOS Software could allow an authenticated, local attacker to inject arbitrary commands that are executed with root privileges. The attacker would need to have Administrator privileges on the device. This vulnerability is due to insufficient input validation of commands supplied by the user. An attacker could exploit this vulnerability by authenticating to a device and submitting crafted input to the affected command. A successful exploit could allow the attacker to execute commands on the underlying operating system with root privileges.	6.7	More Details
CVE-2022-2638	The Export All URLs WordPress plugin before 4.4 does not validate the path of the file to be removed on the system which is supposed to be the CSV file. This could allow high privilege users to delete arbitrary file from the server	6.5	More Details

CVE Number	Description	Base Score	Reference
CVE-2021-46837	res_pjsip_t38 in Sangoma Asterisk 16.x before 16.16.2, 17.x before 17.9.3, and 18.x before 18.2.2, and Certified Asterisk before 16.8-cert7, allows an attacker to trigger a crash by sending an m=image line and zero port in a response to a T.38 re-invite initiated by Asterisk. This is a re-occurrence of the CVE-2019-15297 symptoms but not for exactly the same reason. The crash occurs because there is an append operation relative to the active topology, but this should instead be a replace operation.	6.5	More Details
CVE-2022-36542	An access control issue in the component /ip/admin/ of Edoc-doctor-appointment-system v1.0.1 allows attackers to arbitrarily edit, read, and delete Administrator data.	6.5	More Details
CVE-2022-3017	Cross-Site Request Forgery (CSRF) in GitHub repository froxlor/froxlor prior to 0.10.38.	6.5	More Details
CVE-2022-0669	A flaw was found in dpdk. This flaw allows a malicious vhost-user master to attach an unexpected number of fds as ancillary data to VHOST_USER_GET_INFLIGHT_FD / VHOST_USER_SET_INFLIGHT_FD messages that are not closed by the vhost-user slave. By sending such messages continuously, the vhost-user master exhausts available fd in the vhost-user slave process, leading to a denial of service.	6.5	More Details
CVE-2022-36522	Mikrotik RouterOs through stable v6.48.3 was discovered to contain an assertion failure in the component /advanced-tools/nova/bin/netwatch. This vulnerability allows attackers to cause a Denial of Service (DoS) via a crafted packet.	6.5	More Details
CVE-2022-26529	Realtek Linux/Android Bluetooth Mesh SDK has a buffer overflow vulnerability due to insufficient validation for segmented packets' link parameter. An unauthenticated attacker in the adjacent network can exploit this vulnerability to cause buffer overflow and disrupt service.	6.5	More Details
CVE-2022-26528	Realtek Linux/Android Bluetooth Mesh SDK has a buffer overflow vulnerability due to insufficient validation for the length of segmented packets' shift parameter. An unauthenticated attacker in the adjacent network can exploit this vulnerability to cause buffer overflow and disrupt service.	6.5	More Details
CVE-2022-26527	Realtek Linux/Android Bluetooth Mesh SDK has a buffer overflow vulnerability due to insufficient validation for the size of segmented packets' reference parameter. An unauthenticated attacker in the adjacent network can exploit this vulnerability to cause buffer overflow and disrupt service.	6.5	More Details

CVE Number	Description	Base Score	Reference
CVE-2022-1663	The Stop Spam Comments WordPress plugin through 0.2.1.2 does not properly generate the Javascript access token for preventing abuse of comment section, allowing threat authors to easily collect the value and add it to the request.	6.5	More Details
CVE-2022-25635	Realtek Linux/Android Bluetooth Mesh SDK has a buffer overflow vulnerability due to insufficient validation for broadcast network packet length. An unauthenticated attacker in the adjacent network can exploit this vulnerability to disrupt service.	6.5	More Details
CVE-2022-36687	Ingredients Stock Management System v1.0 was discovered to contain an arbitrary file deletion vulnerability via the component /classes/Master.php?f=delete_img.	6.5	More Details
CVE-2022-2330	Improper Restriction of XML External Entity Reference vulnerability in DLP Endpoint for Windows prior to 11.9.100 allows a remote attacker to cause the DLP Agent to access a local service that the attacker wouldn't usually have access to via a carefully constructed XML file, which the DLP Agent doesn't parse correctly.	6.5	More Details
CVE-2022-37316	Archer Platform 6.8 before 6.11 P3 (6.11.0.3) contains an improper API access control vulnerability in a multi-instance system that could potentially present unauthorized metadata to an authenticated user of the affected system. 6.10 P3 HF1 (6.10.0.3.1) is also a fixed release.	6.5	More Details
CVE-2022-23715	A flaw was discovered in ECE before 3.4.0 that might lead to the disclosure of sensitive information such as user passwords and Elasticsearch keystore settings values in logs such as the audit log or deployment logs in the Logging and Monitoring cluster. The affected APIs are PATCH /api/v1/user and PATCH /deployments/{deployment_id}/elasticsearch/{ref_id}/keystore	6.5	More Details
CVE-2021-4209	A NULL pointer dereference flaw was found in GnuTLS. As Nettle's hash update functions internally call memcpy, providing zero-length input may cause undefined behavior. This flaw leads to a denial of service after authentication in rare circumstances.	6.5	More Details
CVE-2021-3979	A key length flaw was found in Red Hat Ceph Storage. An attacker can exploit the fact that the key length is incorrectly passed in an encryption algorithm to create a non random key, which is weaker and can be exploited for loss of confidentiality and integrity on encrypted disks.	6.5	More Details
CVE-2021-39394	mm-wiki v0.2.1 was discovered to contain a Cross-Site Request Forgery (CSRF) which allows attackers to arbitrarily add user accounts and modify user information.	6.5	More Details

CVE Number	Description	Base Score	Reference
CVE-2022-36945	The Remote Keyless Entry (RKE) receiving unit on certain Mazda vehicles through 2020 allows remote attackers to perform unlock operations and force a resynchronization after capturing three consecutive valid key-fob signals over the radio, aka a RollBack attack. The attacker retains the ability to unlock indefinitely.	6.4	More Details
CVE-2021-35937	A race condition vulnerability was found in rpm. A local unprivileged user could use this flaw to bypass the checks that were introduced in response to CVE-2017-7500 and CVE-2017-7501, potentially gaining root privileges. The highest threat from this vulnerability is to data confidentiality and integrity as well as system availability.	6.4	More Details
CVE-2022-37305	The Remote Keyless Entry (RKE) receiving unit on certain Honda vehicles through 2018 allows remote attackers to perform unlock operations and force a resynchronization after capturing five consecutive valid RKE signals over the radio, aka a RollBack attack. The attacker retains the ability to unlock indefinitely.	6.4	More Details
CVE-2022-37418	The Remote Keyless Entry (RKE) receiving unit on certain Nissan, Kia, and Hyundai vehicles through 2017 allows remote attackers to perform unlock operations and force a resynchronization after capturing two consecutive valid key fob signals over the radio, aka a RollBack attack. The attacker retains the ability to unlock indefinitely.	6.4	More Details
CVE-2022-3013	A vulnerability classified as critical has been found in SourceCodester Simple Task Managing System. This affects an unknown part of the file /loginVaLidation.php. The manipulation of the argument login leads to sql injection. It is possible to initiate the attack remotely. The associated identifier of this vulnerability is VDB-207423.	6.3	More Details
CVE-2022-3012	A vulnerability was found in oretnom23 Fast Food Ordering System. It has been rated as critical. Affected by this issue is some unknown functionality of the file ffos/admin/reports/index.php. The manipulation of the argument date leads to sql injection. The attack may be launched remotely. The exploit has been disclosed to the public and may be used. VDB-207422 is the identifier assigned to this vulnerability.	6.3	More Details
CVE-2022-2957	A vulnerability classified as critical was found in SourceCodester Simple and Nice Shopping Cart Script. Affected by this vulnerability is an unknown functionality of the file /mkshop/Men/profile.php. The manipulation of the argument mem_id leads to sql injection. The attack can be launched remotely. The exploit has been disclosed to the public and may be used. The identifier VDB-207001 was assigned to this vulnerability.	6.3	More Details

CVE Number	Description	Base Score	Reference
CVE-2022-34837	Storing Passwords in a Recoverable Format vulnerability in ABB Zenon 8.20 allows an attacker who successfully exploit the vulnerability may add more network clients that may monitor various activities of the Zenon.	6.2	More Details
CVE-2022-21385	A flaw in net_rds_alloc_sgs() in Oracle Linux kernels allows unprivileged local users to crash the machine. CVSS 3.1 Base Score 6.2 (Availability impacts). CVSS Vector (CVSS:3.1/AV:L/AC:L/PR:N/UI:N/S:U/C:N/I:N/A:H)	6.2	More Details
CVE-2022-36748	PicUploader v2.6.3 was discovered to contain a cross-site scripting (XSS) vulnerability via the component /master/index.php.	6.1	More Details
CVE-2022-2538	The WP Hide & Security Enhancer WordPress plugin before 1.8 does not escape a parameter before outputting it back in an attribute of a backend page, leading to a Reflected Cross-Site Scripting	6.1	More Details
CVE-2022-2599	The Anti-Malware Security and Brute-Force Firewall WordPress plugin before 4.21.83 does not sanitise and escape some parameters before outputting them back in an admin dashboard, leading to Reflected Cross-Site Scripting	6.1	More Details
CVE-2022-36573	A cross-site scripting (XSS) vulnerability in Pagekit CMS v1.0.18 allows attackers to execute arbitrary web scripts or HTML via a crafted payload injected into the Markdown text box under /blog/post/edit.	6.1	More Details
CVE-2022-2537	The WooCommerce PDF Invoices & Packing Slips WordPress plugin before 3.0.1 does not sanitise and escape some parameters before outputting them back in an attributes of an admin page, leading to Reflected Cross-Site Scripting.	6.1	More Details

CVE Number	Description	Base Score	Reference
CVE-2022-36033	jsoup is a Java HTML parser, built for HTML editing, cleaning, scraping, and cross-site scripting (XSS) safety. jsoup may incorrectly sanitize HTML including `javascript:` URL expressions, which could allow XSS attacks when a reader subsequently clicks that link. If the non-default `SafeList.preserveRelativeLinks` option is enabled, HTML including `javascript:` URLs that have been crafted with control characters will not be sanitized. If the site that this HTML is published on does not set a Content Security Policy, an XSS attack is then possible. This issue is patched in jsoup 1.15.3. Users should upgrade to this version. Additionally, as the unsanitized input may have been persisted, old content should be cleaned again using the updated version. To remediate this issue without immediately upgrading: - disable `SafeList.preserveRelativeLinks`, which will rewrite input URLs as absolute URLs - ensure an appropriate [Content Security Policy] (https://developer.mozilla.org/en-US/docs/Web/HTTP/CSP) is defined. (This should be used regardless of upgrading, as a defence-in-depth best practice.)	6.1	More Details
CVE-2022-27547	HCL iNotes is susceptible to a link to non-existent domain vulnerability. An attacker could use this vulnerability to trick a user into supplying sensitive information such as username, password, credit card number, etc.	6.1	More Details
CVE-2022-31798	Nortek Linear eMerge E3-Series 0.32-07p devices are vulnerable to /card_scan.php?CardFormatNo= XSS with session fixation (via PHPSESSID) when they are chained together. This would allow an attacker to take over an admin account or a user account.	6.1	More Details
CVE-2021-3914	It was found that the smallrye health metrics UI component did not properly sanitize some user inputs. An attacker could use this flaw to conduct cross-site scripting attacks.	6.1	More Details
CVE-2022-37161	Claroline 13.5.7 and prior is vulnerable to Cross Site Scripting (XSS) via SVG file upload.	6.1	More Details
CVE-2022-2463	Rockwell Automation ISaGRAF Workbench software versions 6.0 through 6.6.9 are affected by a Path Traversal vulnerability. A crafted malicious .7z exchange file may allow an attacker to gain the privileges of the ISaGRAF Workbench software when opened. If the software is running at the SYSTEM level, then the attacker will gain admin level privileges. User interaction is required for this exploit to be successful.	6.1	More Details

CVE Number	Description	Base Score	Reference
CVE-2021-3427	The Deluge Web-UI is vulnerable to XSS through a crafted torrent file. The the data from torrent files is not properly sanitised as it's interpreted directly as HTML. Someone who supplies the user with a malicious torrent file can execute arbitrary Javascript code in the context of the user's browser session.	6.1	More Details
CVE-2021-39393	mm-wiki v0.2.1 was discovered to contain a cross-site scripting (XSS) vulnerability via the markdown editor.	6.1	More Details
CVE-2022-37153	An issue was discovered in Artica Proxy 4.30.000000. There is a XSS vulnerability via the password parameter in /fw.login.php.	6.1	More Details
CVE-2021-29864	IBM Security Identity Manager 6.0 and 6.0.2 could allow a remote attacker to conduct phishing attacks, using an open redirect attack. By persuading a victim to visit a specially crafted Web site, a remote attacker could exploit this vulnerability to spoof the URL displayed to redirect a user to a malicious Web site that would appear to be trusted. This could allow the attacker to obtain highly sensitive information or conduct further attacks against the victim. IBM X-Force ID: 206089	6.1	More Details
CVE-2022-36745	LibreNMS v22.6.0 was discovered to contain a cross-site scripting (XSS) vulnerability via the component print-customoid.php.	6.1	More Details
CVE-2022-36747	Razor v0.8.0 was discovered to contain a cross-site scripting (XSS) vulnerability via the function uploadchannel().	6.1	More Details
CVE-2022-36746	LibreNMS v22.6.0 was discovered to contain a cross-site scripting (XSS) vulnerability via the component oxidized-cfg-check.inc.php.	6.1	More Details
CVE-2022-36547	Edoc-doctor-appointment-system v1.0.1 was discovered to contain a reflected cross-site scripting (XSS) vulnerability at /patient/index.php. This vulnerability allows attackers to execute arbitrary web scripts or HTML via a crafted payload injected into the Search field.	6.1	More Details
CVE-2022-34368	Dell EMC NetWorker 19.2.1.x 19.3.x, 19.4.x, 19.5.x, 19.6.x and 19.7.0.0 contain an Improper Handling of Insufficient Permissions or Privileges vulnerability. Authenticated non admin user could exploit this vulnerability and gain access to restricted resources.	6.1	More Details

CVE Number	Description	Base Score	Reference
CVE-2022-27560	HCL VersionVault Express exposes administrator credentials.	6.0	More Details
CVE-2021-4158	A NULL pointer dereference issue was found in the ACPI code of QEMU. A malicious, privileged user within the guest could use this flaw to crash the QEMU process on the host, resulting in a denial of service condition.	6.0	More Details
CVE-2022-34836	Relative Path Traversal vulnerability in ABB Zenon 8.20 allows the user to access files on the Zenon system and user also can add own log messages and e.g., flood the log entries. An attacker who successfully exploit the vulnerability could access the Zenon runtime activities such as the start and stop of various activity and the last error code etc.	5.9	More Details
CVE-2022-27558	HCL iNotes is susceptible to a Broken Password Strength Checks vulnerability. Custom password policies are not enforced on certain iNotes forms which could allow users to set weak passwords, leading to easier cracking.	5.9	More Details
CVE-2021-43309	An exponential ReDoS (Regular Expression Denial of Service) can be triggered in the uri-template-lite npm package, when an attacker is able to supply arbitrary input to the "URI.expand" method	5.9	More Details
CVE-2021-43767	Odyssey passes to client unencrypted bytes from man-in-the-middle When Odyssey storage is configured to use the PostgreSQL server using 'trust' authentication with a 'clientcert' requirement or to use 'cert' authentication, a man-in-the-middle attacker can inject false responses to the client's first few queries. Despite the use of SSL certificate verification and encryption, Odyssey will pass these results to client as if they originated from valid server. This is similar to CVE-2021-23222 for PostgreSQL.	5.9	More Details

CVE Number	Description	Base Score	Reference
CVE-2022-36037	kirby is a content management system (CMS) that adapts to many different projects and helps you build your own ideal interface. Cross-site scripting (XSS) is a type of vulnerability that allows execution of any kind of JavaScript code inside the Panel session of the same or other users. In the Panel, a harmful script can for example trigger requests to Kirby's API with the permissions of the victim. If bad actors gain access to your group of authenticated Panel users they can escalate their privileges via the Panel session of an admin user. Depending on your site, other JavaScript-powered attacks are possible. The multiselect field allows selection of tags from an autocompleted list. Unfortunately, the Panel in Kirby 3.5 used HTML rendering for the raw option value. This allowed **attackers with influence on the options source** to store HTML code. The browser of the victim who visited a page with manipulated multiselect options in the Panel will then have rendered this malicious HTML code when the victim opened the autocomplete dropdown. Users are *not* affected by this vulnerability if you don't use the multiselect field or don't use it with options that can be manipulated by attackers. The problem has been patched in Kirby 3.5.8.1.	5.9	More Details
CVE-2022-1198	A use-after-free vulnerabilitity was discovered in drivers/net/hamradio/6pack.c of linux that allows an attacker to crash linux kernel by simulating ax25 device using 6pack driver from user space.	5.5	More Details
CVE-2022-0480	A flaw was found in the filelock_init in fs/locks.c function in the Linux kernel. This issue can lead to host memory exhaustion due to memcg not limiting the number of Portable Operating System Interface (POSIX) file locks.	5.5	More Details
CVE-2022-0496	A vulnerbiility was found in Openscad, where a DXF-format drawing with particular (not necessarily malformed!) properties may cause an out-of-bounds memory access when imported using import().	5.5	More Details
CVE-2022-0851	There is a flaw in convert2rhel. When the --activationkey option is used with convert2rhel, the activation key is subsequently passed to subscription-manager via the command line, which could allow unauthorized users locally on the machine to view the activation key via the process command line via e.g. htop or ps. The specific impact varies upon the subscription, but generally this would allow an attacker to register systems purchased by the victim until discovered; a form of fraud. This could occur regardless of how the activation key is supplied to convert2rhel because it involves how convert2rhel provides it to subscription-manager.	5.5	More Details

CVE Number	Description	Base Score	Reference
CVE-2022-0852	There is a flaw in convert2rhel. convert2rhel passes the Red Hat account password to subscription-manager via the command line, which could allow unauthorized users locally on the machine to view the password via the process command line via e.g. htop or ps. The specific impact varies upon the privileges of the Red Hat account in question, but it could affect the integrity, availability, and/or data confidentiality of other systems that are administered by that account. This occurs regardless of how the password is supplied to convert2rhel.	5.5	More Details
CVE-2022-1016	A flaw was found in the Linux kernel in net/netfilter/nf_tables_core.c:nft_do_chain, which can cause a use-after-free. This issue needs to handle 'return' with proper preconditions, as it can lead to a kernel information leak problem caused by a local, unprivileged attacker.	5.5	More Details
CVE-2021-4022	A vulnerability was found in rizin. The bug involves an ELF64 binary for the HPPA architecture. When a specially crafted binarygets analysed by rizin, it causes rizin to crash by freeing an uninitialized (and potentially user controlled, depending on the build) memory address.	5.5	More Details
CVE-2022-1115	A heap-buffer-overflow flaw was found in ImageMagick's PushShortPixel() function of quantum-private.h file. This vulnerability is triggered when an attacker passes a specially crafted TIFF image file to ImageMagick for conversion, potentially leading to a denial of service.	5.5	More Details
CVE-2022-35020	Advancecomp v2.3 was discovered to contain a heap buffer overflow via the component __interceptor_memcpy at /sanitizer_common/sanitizer_common_interceptors.inc.	5.5	More Details
CVE-2022-35019	Advancecomp v2.3 was discovered to contain a segmentation fault.	5.5	More Details
CVE-2022-1184	A use-after-free flaw was found in fs/ext4/namei.c:dx_insert_block() in the Linux kernel's filesystem sub-component. This flaw allows a local attacker with a user privilege to cause a denial of service.	5.5	More Details
CVE-2022-2569	The affected device stores sensitive information in cleartext, which may allow an authenticated user to access session data stored in the OAuth database belonging to legitimate users	5.5	More Details
CVE-2022-1204	A use-after-free flaw was found in the Linux kernel's Amateur Radio AX.25 protocol functionality in the way a user connects with the protocol. This flaw allows a local user to crash the system.	5.5	More Details

CVE Number	Description	Base Score	Reference
CVE-2022-2953	LibTIFF 4.4.0 has an out-of-bounds read in extractImageSection in tools/tiffcrop.c:6905, allowing attackers to cause a denial-of-service via a crafted tiff file. For users that compile libtiff from sources, the fix is available with commit 48d6ece8.	5.5	More Details
CVE-2022-33172	de.fac2 1.34 allows bypassing the User Presence protection mechanism when there is malware on the victim's PC.	5.5	More Details
CVE-2022-37292	Tenda AX12 V22.03.01.21_CN is vulnerable to Buffer Overflow. This overflow is triggered in the sub_42FDE4 function, which satisfies the request of the upper-level interface function sub_430124, that is, handles the post request under /goform/SetIpMacBind.	5.5	More Details
CVE-2021-0698	In PVRSRVBridgeHeapCfgHeapDetails, there is a possible leak of kernel heap content due to uninitialized data. This could lead to local information disclosure with no additional execution privileges needed. User interaction is not needed for exploitation.Product: AndroidVersions: Android SoCAndroid ID: A-236848165	5.5	More Details
CVE-2022-36561	XPDF v4.0.4 was discovered to contain a segmentation violation via the component /xpdf/AcroForm.cc:538.	5.5	More Details
CVE-2021-0887	In PVRSRVBridgeHeapCfgHeapConfigName, there is a possible leak of kernel heap content due to uninitialized data. This could lead to local information disclosure with no additional execution privileges needed. User interaction is not needed for exploitation.Product: AndroidVersions: Android SoCAndroid ID: A-236848817	5.5	More Details
CVE-2021-4142	The Candlepin component of Red Hat Satellite was affected by an improper authentication flaw. Few factors could allow an attacker to use the SCA (simple content access) certificate for authentication with Candlepin.	5.5	More Details
CVE-2021-4155	A data leak flaw was found in the way XFS_IOC_ALLOCSP IOCTL in the XFS filesystem allowed for size increase of files with unaligned size. A local attacker could use this flaw to leak data on the XFS filesystem otherwise not accessible to them.	5.5	More Details
CVE-2022-35017	Advancecomp v2.3 was discovered to contain a heap buffer overflow.	5.5	More Details

CVE Number	Description	Base Score	Reference
CVE-2022-32838	A logic issue was addressed with improved state management. This issue is fixed in macOS Monterey 12.5, macOS Big Sur 11.6.8, Security Update 2022-005 Catalina, iOS 15.6 and iPadOS 15.6. An app may be able to read arbitrary files.	5.5	More Details
CVE-2021-4214	A heap overflow flaw was found in libpngs' pngimage.c program. This flaw allows an attacker with local network access to pass a specially crafted PNG file to the pngimage utility, causing an application to crash, leading to a denial of service.	5.5	More Details
CVE-2022-32834	An access issue was addressed with improvements to the sandbox. This issue is fixed in macOS Monterey 12.5, macOS Big Sur 11.6.8, Security Update 2022-005 Catalina. An app may be able to access sensitive user information.	5.5	More Details
CVE-2021-4218	A flaw was found in the Linux kernel’s implementation of reading the SVC RDMA counters. Reading the counter sysctl panics the system. This flaw allows a local attacker with local access to cause a denial of service while the system reboots. The issue is specific to CentOS/RHEL.	5.5	More Details
CVE-2022-35018	Advancecomp v2.3 was discovered to contain a segmentation fault.	5.5	More Details
CVE-2021-4216	A Floating point exception (division-by-zero) flaw was found in Mupdf for zero width pages in muraster.c. It is fixed in Mupdf-1.20.0-rc1 upstream.	5.5	More Details
CVE-2022-35016	Advancecomp v2.3 was discovered to contain a heap buffer overflow.	5.5	More Details
CVE-2020-27797	An invalid memory address reference was discovered in the elf_lookup function in p_lx_elf.cpp in UPX 4.0.0 via a crafted Mach-O file.	5.5	More Details
CVE-2022-38533	In GNU Binutils before 2.40, there is a heap-buffer-overflow in the error function bfd_getl32 when called from the strip_main function in strip-new via a crafted file.	5.5	More Details
CVE-2022-2980	NULL Pointer Dereference in GitHub repository vim/vim prior to 9.0.0259.	5.5	More Details
CVE-2021-33844	A floating point exception (divide-by-zero) issue was discovered in SoX in functon startread() of wav.c file. An attacker with a crafted wav file, could cause an application to crash.	5.5	More Details

CVE Number	Description	Base Score	Reference
CVE-2021-23210	A floating point exception (divide-by-zero) issue was discovered in SoX in functon read_samples() of voc.c file. An attacker with a crafted file, could cause an application to crash.	5.5	More Details
CVE-2021-23172	A vulnerability was found in SoX, where a heap-buffer-overflow occurs in function startread() in hcom.c file. The vulnerability is exploitable with a crafted hcomn file, that could cause an application to crash.	5.5	More Details
CVE-2021-23159	A vulnerability was found in SoX, where a heap-buffer-overflow occurs in function lsx_read_w_buf() in formats_i.c file. The vulnerability is exploitable with a crafted file, that could cause an application to crash.	5.5	More Details
CVE-2021-40326	Foxit PDF Reader before 11.1 and PDF Editor before 11.1, and PhantomPDF before 10.1.6, mishandle hidden and incremental data in signed documents. An attacker can write to an arbitrary file, and display controlled contents, during signature verification.	5.5	More Details
CVE-2021-20224	An integer overflow issue was discovered in ImageMagick's ExportIndexQuantum() function in MagickCore/quantum-export.c. Function calls to GetPixelIndex() could result in values outside the range of representable for the 'unsigned char'. When ImageMagick processes a crafted pdf file, this could lead to an undefined behaviour or a crash.	5.5	More Details
CVE-2021-3585	A flaw was found in openstack-tripleo-heat-templates. Plain passwords from RHSM exist in the logs during OSP13 deployment with subscription-manager.	5.5	More Details
CVE-2020-27802	An floating point exception was discovered in the elf_lookup function in p_lx_elf.cpp in UPX 4.0.0 via a crafted Mach-O file.	5.5	More Details
CVE-2020-27798	An invalid memory address reference was discovered in the adjABS function in p_lx_elf.cpp in UPX 4.0.0 via a crafted Mach-O file.	5.5	More Details
CVE-2021-3669	A flaw was found in the Linux kernel. Measuring usage of the shared memory does not scale with large shared memory segment counts which could lead to resource exhaustion and DoS.	5.5	More Details
CVE-2022-38791	In MariaDB before 10.9.2, compress_write in extra/mariabackup/ds_compress.cc does not release data_mutex upon a stream write failure, which allows local users to trigger a deadlock.	5.5	More Details

CVE Number	Description	Base Score	Reference
CVE-2022-0175	A flaw was found in the VirGL virtual OpenGL renderer (virglrenderer). The virgl did not properly initialize memory when allocating a host-backed memory resource. A malicious guest could use this flaw to mmap from the guest kernel and read this uninitialized memory from the host, possibly leading to information disclosure.	5.5	More Details
CVE-2022-0171	A flaw was found in the Linux kernel. The existing KVM SEV API has a vulnerability that allows a non-root (host) user-level application to crash the host kernel by creating a confidential guest VM instance in AMD CPU that supports Secure Encrypted Virtualization (SEV).	5.5	More Details
CVE-2022-35014	Advancecomp v2.3 contains a segmentation fault.	5.5	More Details
CVE-2022-35015	Advancecomp v2.3 was discovered to contain a heap buffer overflow via le_uint32_read at /lib/endianrw.h.	5.5	More Details
CVE-2022-25641	Foxit PDF Reader before 11.2.2 and PDF Editor before 11.2.2, and PhantomPDF before 10.1.8, mishandle cross-reference information during compressed-object parsing within signed documents. This leads to delivery of incorrect signature information via an Incremental Saving Attack and a Shadow Attack.	5.5	More Details
CVE-2022-36358	Cross-Site Request Forgery (CSRF) vulnerability in SEO Scout plugin <= 0.9.83 at WordPress allows attackers to trick users with administrative rights to unintentionally change the plugin settings.	5.4	More Details
CVE-2022-36527	Jfinal CMS v5.1.0 allows attackers to execute arbitrary web scripts or HTML via a crafted payload injected into the post title text field under the publish blog module.	5.4	More Details
CVE-2022-37239	MDaemon Technologies SecurityGateway for Email Servers 8.5.2 is vulnerable to Cross Site Scripting (XSS) via the rulles_list_ajax endpoint.	5.4	More Details
CVE-2022-37241	MDaemon Technologies SecurityGateway for Email Servers 8.5.2 is vulnerable to Cross Site Scripting (XSS) via the data_leak_list_ajax endpoint.	5.4	More Details
CVE-2022-37243	MDaemon Technologies SecurityGateway for Email Servers 8.5.2 is vulnerable to Cross Site Scripting (XSS) via the whitelist endpoint.	5.4	More Details

CVE Number	Description	Base Score	Reference
CVE-2022-37244	MDaemon Technologies SecurityGateway for Email Servers 8.5.2 is vulnerable to IFRAME Injectionvia the currentRequest parameter. after login leads to inject malicious tag leads to IFRAME injection.	5.4	More Details
CVE-2022-37245	MDaemon Technologies SecurityGateway for Email Servers 8.5.2 is vulnerable to Cross Site Scripting (XSS) via the Blacklist endpoint.	5.4	More Details
CVE-2022-33935	Dell EMC Data Protection Advisor versions 19.6 and earlier, contains a Stored Cross Site Scripting, an attacker could potentially exploit this vulnerability, leading to the storage of malicious HTML or JavaScript codes in a trusted application data store. When a victim user accesses the data store through their browsers, the malicious code gets executed by the web browser in the context of the vulnerable web application. Exploitation may lead to information disclosure, session theft, or client-side request forgery.	5.4	More Details
CVE-2021-38934	IBM Engineering Test Management 7.0, 7.0.1, and 7.0.2 is vulnerable to cross-site scripting. This vulnerability allows users to embed arbitrary JavaScript code in the Web UI thus altering the intended functionality potentially leading to credentials disclosure within a trusted session. IBM X-Force ID: 210671.	5.4	More Details
CVE-2022-37238	MDaemon Technologies SecurityGateway for Email Servers 8.5.2 is vulnerable to Cross Site Scripting (XSS) via the currentRequest parameter.	5.4	More Details
CVE-2022-37160	Claroline 13.5.7 and prior allows an authenticated attacker to elevate privileges via the arbitrary creation of a privileged user. By combining the XSS vulnerability present in several upload forms and a javascript request to the present API, it is possible to trigger the creation of a user with administrative rights by opening an SVG file as an administrator user.	5.4	More Details
CVE-2022-31677	An Insufficient Session Expiration issue was discovered in the Pinniped Supervisor (before v0.19.0). A user authenticating to Kubernetes clusters via the Pinniped Supervisor could potentially use their access token to continue their session beyond what proper use of their refresh token might allow.	5.4	More Details
CVE-2022-32746	A flaw was found in the Samba AD LDAP server. The AD DC database audit logging module can access LDAP message values freed by a preceding database module, resulting in a use-after-free issue. This issue is only possible when modifying certain privileged attributes, such as userAccountControl.	5.4	More Details

CVE Number	Description	Base Score	Reference
CVE-2022-35714	IBM Maximo Asset Management 7.6.1 is vulnerable to cross-site scripting. This vulnerability allows users to embed arbitrary JavaScript code in the Web UI thus altering the intended functionality potentially leading to credentials disclosure within a trusted session. IBM X-Force ID: 231116.	5.4	More Details
CVE-2022-37162	Claroline 13.5.7 and prior is vulnerable to Cross Site Scripting (XSS). An attacker can obtain javascript code execution by adding arbitrary javascript code in the 'Location' field of a calendar event.	5.4	More Details
CVE-2022-36194	Centreon 22.04.0 is vulnerable to Cross Site Scripting (XSS) from the function Pollers > Broker Configuration by adding a crafted payload into the name parameter.	5.4	More Details
CVE-2022-37150	An issue was discovered in Online Diagnostic Lab Management System 1.0. There is a stored XSS vulnerability via firstname, address, middlename, lastname , gender, email, contact parameters.	5.4	More Details
CVE-2022-36548	Edoc-doctor-appointment-system v1.0.1 was discovered to contain a stored cross-site scripting (XSS) vulnerability at /patient/settings.php. This vulnerability allows attackers to execute arbitrary web scripts or HTML via a crafted payload injected into the Name text field.	5.4	More Details
CVE-2018-14520	An issue was discovered in Kirby 2.5.12. The application allows malicious HTTP requests to be sent in order to trick a user into adding web pages.	5.4	More Details
CVE-2022-38080	Reflected cross-site scripting vulnerability in Exment ((PHP8) exceedone/exment v5.0.2 and earlier and exceedone/laravel-admin v3.0.0 and earlier, (PHP7) exceedone/exment v4.4.2 and earlier and exceedone/laravel-admin v2.2.2 and earlier) allows a remote authenticated attacker to inject an arbitrary script.	5.4	More Details
CVE-2022-0225	A flaw was found in Keycloak. This flaw allows a privileged attacker to use the malicious payload as the group name while creating a new group from the admin console, leading to a stored Cross-site scripting (XSS) attack.	5.4	More Details
CVE-2022-25646	All versions of package x-data-spreadsheet are vulnerable to Cross-site Scripting (XSS) due to missing sanitization of values inserted into the cells.	5.4	More Details
CVE-2022-38089	Stored cross-site scripting vulnerability in Exment ((PHP8) exceedone/exment v5.0.2 and earlier and exceedone/laravel-admin v3.0.0 and earlier, (PHP7) exceedone/exment v4.4.2 and earlier and exceedone/laravel-admin v2.2.2 and earlier) allows a remote authenticated attacker to inject an arbitrary script.	5.4	More Details

CVE Number	Description	Base Score	Reference
CVE-2022-2034	The Sensei LMS WordPress plugin before 4.5.0 does not have proper permissions set in one of its REST endpoint, allowing unauthenticated users to access private messages sent to teachers	5.3	More Details
CVE-2022-2373	The Simply Schedule Appointments WordPress plugin before 1.5.7.7 is missing authorisation in a REST endpoint, allowing unauthenticated users to retrieve WordPress users details such as name and email address	5.3	More Details
CVE-2022-25887	The package sanitize-html before 2.7.1 are vulnerable to Regular Expression Denial of Service (ReDoS) due to insecure global regular expression replacement logic of HTML comment removal.	5.3	More Details
CVE-2022-36121	An issue was discovered in Blue Prism Enterprise 6.0 through 7.01. In a misconfigured environment that exposes the Blue Prism Application server, it is possible for an authenticated user to reverse engineer the Blue Prism software and circumvent access controls for the UpdateOfflineHelpData administrative function. Abusing this function will allow any Blue Prism user to change the offline help URL to one of their choice, opening the possibility of spoofing the help page or executing a local file.	5.3	More Details
CVE-2022-36118	An issue was discovered in Blue Prism Enterprise 6.0 through 7.01. In a misconfigured environment that exposes the Blue Prism Application server, it is possible for an authenticated user to reverse engineer the Blue Prism software and circumvent access controls for the SetProcessAttributes administrative function. Abusing this function will allow any Blue Prism user to publish, unpublish, or retire processes. Using this function, any logged-in user can change the status of a process, an action allowed only intended for users with the Edit Process permission.	5.3	More Details
CVE-2021-3754	A flaw was found in keycloak where an attacker is able to register himself with the username same as the email ID of any existing user. This may cause trouble in getting password recovery email in case the user forgets the password.	5.3	More Details
CVE-2022-36116	An issue was discovered in Blue Prism Enterprise 6.0 through 7.01. In a misconfigured environment that exposes the Blue Prism Application server, it is possible for an authenticated user to reverse engineer the Blue Prism software and circumvent access controls for the setValidationInfo administrative function. Removing the validation applied to newly designed processes increases the chance of successfully hiding malicious code that could be executed in a production environment.	5.3	More Details

CVE Number	Description	Base Score	Reference
CVE-2022-23235	Active IQ Unified Manager for VMware vSphere, Linux, and Microsoft Windows versions prior to 9.10P1 are susceptible to a vulnerability which could allow an attacker to discover cluster, node and Active IQ Unified Manager specific information via AutoSupport telemetry data that is sent even when AutoSupport has been disabled.	5.3	More Details
CVE-2021-4189	A flaw was found in Python, specifically in the FTP (File Transfer Protocol) client library in PASV (passive) mode. The issue is how the FTP client trusts the host from the PASV response by default. This flaw allows an attacker to set up a malicious FTP server that can trick FTP clients into connecting back to a given IP address and port. This vulnerability could lead to FTP client scanning ports, which otherwise would not have been possible.	5.3	More Details
CVE-2021-4040	A flaw was found in AMQ Broker. This issue can cause a partial interruption to the availability of AMQ Broker via an Out of memory (OOM) condition. This flaw allows an attacker to partially disrupt availability to the broker through a sustained attack of maliciously crafted messages. The highest threat from this vulnerability is system availability.	5.3	More Details
CVE-2021-32570	In Ericsson Network Manager (ENM) releases before 21.2, users belonging to the same AMOS authorization group can retrieve the data from certain log files. All AMOS users are considered to be highly privileged users in ENM system and all must be previously defined and authorized by the Security Administrator. Those users can access some log’s files, under a common path, and read information stored in the log’s files in order to conduct privilege escalation.	4.9	More Details
CVE-2022-0718	A flaw was found in python-oslo-utils. Due to improper parsing, passwords with a double quote (") in them cause incorrect masking in debug logs, causing any part of the password after the double quote to be plaintext.	4.9	More Details
CVE-2022-3035	Cross-site Scripting (XSS) - Stored in GitHub repository snipe/snipe-it prior to v6.0.11.	4.8	More Details
CVE-2022-37059	Cross Site Scripting (XSS) in Admin Panel of Subrion CMS 4.2.1 allows attacker to inject arbitrary code via Login Field	4.8	More Details
CVE-2022-36657	Library Management System v1.0 was discovered to contain a cross-site scripting (XSS) vulnerability via the component /librarian/edit_book_details.php.	4.8	More Details

CVE Number	Description	Base Score	Reference
CVE-2022-0485	A flaw was found in the copying tool `nbdcopy` of libnbd. When performing multi-threaded copies using asynchronous nbd calls, nbdcopy was blindly treating the completion of an asynchronous command as successful, rather than checking the *error parameter. This could result in the silent creation of a corrupted destination image.	4.8	More Details
CVE-2021-3688	A flaw was found in Red Hat JBoss Core Services HTTP Server in all versions, where it does not properly normalize the path component of a request URL contains dot-dot-semicolon(s). This flaw could allow an attacker to access unauthorized information or possibly conduct further attacks. The highest threat from this vulnerability is to data confidentiality and integrity.	4.8	More Details
CVE-2022-2374	The Simply Schedule Appointments WordPress plugin before 1.5.7.7 does not sanitise and escape some of its settings, which could allow high privilege users such as admin to perform Stored Cross-Site Scripting attacks even when the unfiltered_html capability is disallowed (for example in multisite setup)	4.8	More Details
CVE-2022-37952	A reflected cross-site scripting (XSS) vulnerability exists in the iHistorian Data Display of WorkstationST (<v07.09.15) could allow an attacker to compromise a victim's browser. WorkstationST is only deployed in specific, controlled environments rendering attack complexity significantly higher than if the attack were conducted on the software in isolation. WorkstationST v07.09.15 can be found in ControlST v07.09.07 SP8 and greater.	4.7	More Details
CVE-2022-37953	An HTTP response splitting vulnerability exists in the AM Gateway Challenge-Response dialog of WorkstationST (<v07.09.15) and could allow an attacker to compromise a victim's browser/session. WorkstationST is only deployed in specific, controlled environments rendering attack complexity significantly higher than if the attack were conducted on the software in isolation. WorkstationST v07.09.15 can be found in ControlST v07.09.07 SP8 and greater.	4.7	More Details
CVE-2022-0207	A race condition was found in vdsm. Functionality to obfuscate sensitive values in log files that may lead to values being stored in clear text.	4.7	More Details
CVE-2021-4159	A vulnerability was found in the Linux kernel's EBPF verifier when handling internal data structures. Internal memory locations could be returned to userspace. A local attacker with the permissions to insert eBPF code to the kernel can use this to leak internal kernel memory details defeating some of the exploit mitigations in place for the kernel.	4.4	More Details

CVE Number	Description	Base Score	Reference
CVE-2022-0216	A use-after-free vulnerability was found in the LSI53C895A SCSI Host Bus Adapter emulation of QEMU. The flaw occurs while processing repeated messages to cancel the current SCSI request via the lsi_do_msgout function. This flaw allows a malicious privileged user within the guest to crash the QEMU process on the host, resulting in a denial of service.	4.4	More Details
CVE-2021-3735	A deadlock issue was found in the AHCI controller device of QEMU. It occurs on a software reset (ahci_reset_port) while handling a host-to-device Register FIS (Frame Information Structure) packet from the guest. A privileged user inside the guest could use this flaw to hang the QEMU process on the host, resulting in a denial of service condition. The highest threat from this vulnerability is to system availability.	4.4	More Details
CVE-2022-0168	A denial of service (DOS) issue was found in the Linux kernel's smb2_ioctl_query_info function in the fs/cifs/smb2ops.c Common Internet File System (CIFS) due to an incorrect return from the memdup_user function. This flaw allows a local, privileged (CAP_SYS_ADMIN) attacker to crash the system.	4.4	More Details
CVE-2022-2787	Schroot before 1.6.13 had too permissive rules on chroot or session names, allowing a denial of service on the schroot service for all users that may start a schroot session.	4.3	More Details
CVE-2021-3856	ClassLoaderTheme and ClasspathThemeResourceProviderFactory allows reading any file available as a resource to the classloader. By sending requests for theme resources with a relative path from an external HTTP client, the client will receive the content of random files if available.	4.3	More Details
CVE-2021-4122	It was found that a specially crafted LUKS header could trick cryptsetup into disabling encryption during the recovery of the device. An attacker with physical access to the medium, such as a flash disk, could use this flaw to force a user into permanently disabling the encryption layer of that medium.	4.3	More Details
CVE-2022-32857	This issue was addressed by using HTTPS when sending information over the network. This issue is fixed in macOS Monterey 12.5, macOS Big Sur 11.6.8, Security Update 2022-005 Catalina, iOS 15.6 and iPadOS 15.6, tvOS 15.6, watchOS 8.7. A user in a privileged network position can track a user's activity.	4.3	More Details

CVE Number	Description	Base Score	Reference
CVE-2022-2080	The Sensei LMS WordPress plugin before 4.5.2 does not ensure that the sender of a private message is either the teacher or the original sender, allowing any authenticated user to send messages to arbitrary private conversation via a IDOR attack. Note: Attackers are not able to see responses/messages between the teacher and student	4.3	More Details
CVE-2018-14519	An issue was discovered in Kirby 2.5.12. The delete page functionality suffers from a CSRF flaw. A remote attacker can craft a malicious CSRF page and force the user to delete a page.	4.3	More Details
CVE-2022-32742	A flaw was found in Samba. Some SMB1 write requests were not correctly range-checked to ensure the client had sent enough data to fulfill the write, allowing server memory contents to be written into the file (or printer) instead of client-supplied data. The client cannot control the area of the server memory written to the file (or printer).	4.3	More Details
CVE-2022-2267	The Mailchimp for WooCommerce WordPress plugin before 2.7.1 has an AJAX action that allows any logged in users (such as subscriber) to perform a POST request on behalf of the server to the internal network/LAN, the body of the request is also appended to the response so it can be used to scan private network for example	4.3	More Details
CVE-2022-0812	An information leak flaw was found in NFS over RDMA in the net/sunrpc/xprtrdma/rpc_rdma.c in the Linux Kernel. This flaw allows an attacker with normal user privileges to leak kernel information.	4.3	More Details
CVE-2022-36036	mdx-mermaid provides plug and play access to Mermaid in MDX. There is a potential for an arbitrary javascript injection in versions less than 1.3.0 and 2.0.0-rc1. Modify any mermaid code blocks with arbitrary code and it will execute when the component is loaded by MDXjs. This vulnerability was patched in version(s) 1.3.0 and 2.0.0-rc2. There are currently no known workarounds.	3.6	More Details
CVE-2022-3015	A vulnerability, which was classified as problematic, has been found in oretnom23 Fast Food Ordering System. This issue affects some unknown processing of the file admin/?page=reports. The manipulation of the argument date leads to cross site scripting. The attack may be initiated remotely. The identifier VDB-207425 was assigned to this vulnerability.	3.5	More Details
CVE-2022-3014	A vulnerability classified as problematic was found in SourceCodester Simple Task Managing System. This vulnerability affects unknown code. The manipulation of the argument student_add leads to cross site scripting. The attack can be initiated remotely. The identifier of this vulnerability is VDB-207424.	3.5	More Details

CVE Number	Description	Base Score	Reference
CVE-2021-4217	A flaw was found in unzip. The vulnerability occurs due to improper handling of Unicode strings, which can lead to a null pointer dereference. This flaw allows an attacker to input a specially crafted zip file, leading to a crash or code execution.	3.3	More Details
CVE-2021-3574	A vulnerability was found in ImageMagick-7.0.11-5, where executing a crafted file with the convert command, ASAN detects memory leaks.	3.3	More Details
CVE-2021-3644	A flaw was found in wildfly-core in all versions. If a vault expression is in the form of a single attribute that contains multiple expressions, a user who was granted access to the management interface can potentially access a vault expression they should not be able to access and possibly retrieve the item which was stored in the vault. The highest threat from this vulnerability is data confidentiality and integrity.	3.3	More Details
CVE-2022-36117	An issue was discovered in Blue Prism Enterprise 6.0 through 7.01. In a misconfigured environment that exposes the Blue Prism Application server, it is possible for an authenticated user to reverse engineer the Blue Prism software and circumvent access controls for an administrative function. If credential access is configured to be accessible by a machine or the runtime resource security group, using further reverse engineering, an attacker can spoof a known machine and request known encrypted credentials to decrypt later.	3.1	More Details
CVE-2022-2556	The Mailchimp for WooCommerce WordPress plugin before 2.7.2 has an AJAX action that allows high privilege users to perform a POST request on behalf of the server to the internal network/LAN, the body of the request is also appended to the response so it can be used to scan private network for example	2.7	More Details
CVE-2022-36168	A directory traversal vulnerability was discovered in Wuzhicms 4.1.0. via /coreframe/app/attachment/admin/index.php:	2.7	More Details
CVE-2022-3022	Rejected reason: DO NOT USE THIS CANDIDATE NUMBER. Reason: This CVE has been rejected as it was incorrectly assigned. All references and descriptions in this candidate have been removed to prevent accidental usage	N/A	More Details
CVE-2021-4042	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

CVE Number	Description	Base Score	Reference
CVE-2022-36707	Rejected reason: DO NOT USE THIS CANDIDATE NUMBER. ConsultIDs: CVE-2022-2214. Reason: This candidate is a reservation duplicate of CVE-2022-2214. Notes: All CVE users should reference CVE-2022-2214 instead of this candidate. All references and descriptions in this candidate have been removed to prevent accidental usage	N/A	More Details
CVE-2022-24304	Rejected reason: DO NOT USE THIS CANDIDATE NUMBER. ConsultIDs: CVE-2022-2564. Reason: This candidate is a duplicate of CVE-2022-2564. Notes: All CVE users should reference CVE-2022-2564 instead of this candidate. All references and descriptions in this candidate have been removed to prevent accidental usage	N/A	More Details
CVE-2018-5483	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
CVE-2018-5494	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
CVE-2021-4215	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
CVE-2022-1024	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
CVE-2021-3913	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
CVE-2021-4141	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
CVE-2021-20223	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
CVE-2021-20258	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
CVE-2021-20192	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

CVE Number	Description	Base Score	Reference
CVE-2021-3651	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
CVE-2021-3627	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
CVE-2021-3691	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
CVE-2020-35520	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
CVE-2021-20301	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
CVE-2021-3488	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
CVE-2022-38785	Rejected reason: DO NOT USE THIS CANDIDATE NUMBER. ConsultIDs: CVE-2022-2905. Reason: This candidate is a reservation duplicate of CVE-2022-2905. Notes: All CVE users should reference CVE-2022-2905 instead of this candidate. All references and descriptions in this candidate have been removed to prevent accidental usage	N/A	More Details
CVE-2022-0644	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
CVE-2021-20287	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
CVE-2022-3063	Rejected reason: DO NOT USE THIS CANDIDATE NUMBER. Reason: This CVE has been rejected as it was incorrectly assigned. All references and descriptions in this candidate have been removed to prevent accidental usage	N/A	More Details