SingCERT
Singapore Cyber Emergency Response Team

Security Bulletin 27 September 2023

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-2023-2163	Incorrect verifier pruning in BPF in Linux Kernel >=5.4 leads to unsafe code paths being incorrectly marked as safe, resulting in arbitrary read/write in kernel memory, lateral privilege escalation, and container escape.	10.0	More Details
CVE-2023-43240	D-Link DIR-816 A2 v1.10CNB05 was discovered to contain a stack overflow via parameter sip_address in ipportFilter.	9.8	More Details
CVE-2023-31719	FUXA <= 1.1.12 is vulnerable to SQL Injection via /api/signin.	9.8	More Details
CVE-2023-43130	D-LINK DIR-806 1200M11AC wireless router DIR806A1_FW100CNb11 is vulnerable to command injection.	9.8	More Details
CVE-2023-43129	D-LINK DIR-806 1200M11AC wireless router DIR806A1_FW100CNb11 is vulnerable to command injection due to lax filtering of REMOTE_PORT parameters.	9.8	More Details

CVE Number	Description	Base Score	Reference
CVE-2023-40989	SQL injection vulnerbility in jeecgboot jeecg-boot v 3.0, 3.5.3 that allows a remote attacker to execute arbitrary code via a crafted request to the report/jeecgboot/jmreport/queryFieldBySql component.	9.8	More Details
CVE-2023-43270	dst-admin v1.5.0 was discovered to contain a remote command execution (RCE) vulnerability via the userId parameter at /home/playerOperate.	9.8	More Details
CVE-2023-43144	Projectworldsl Assets-management-system-in-php 1.0 is vulnerable to SQL Injection via the "id" parameter in delete.php.	9.8	More Details
CVE-2023-43762	Certain WithSecure products allow Unauthenticated Remote Code Execution via the web server (backend). This affects WithSecure Policy Manager 15 and Policy Manager Proxy 15.	9.8	More Details
CVE-2023-43128	D-LINK DIR-806 1200M11AC wireless router DIR806A1_FW100CNb11 is vulnerable to command injection due to lax filtering of HTTP_ST parameters.	9.8	More Details
CVE-2023-43468	SQL injection vulnerability in janobe Online Job Portal v.2020 allows a remote attacker to execute arbitrary code via the login.php component.	9.8	More Details
CVE-2023-34576	SQL injection vulnerability in updatepos.php in PrestaShop opartfaq through 1.0.3 allows remote attackers to run arbitrary SQL commands via unspedified vector.	9.8	More Details
CVE-2023-42810	systeminformation is a System Information Library for Node.JS. Versions 5.0.0 through 5.21.6 have a SSID Command Injection Vulnerability. The problem was fixed with a parameter check in version 5.21.7. As a workaround, check or sanitize parameter strings that are passed to `wifiConnections()`, `wifiNetworks()` (string only).	9.8	More Details
CVE-2023-42279	Dreamer CMS v4.1.3 was discovered to contain a SQL injection vulnerability via the model-form-management-field form.	9.8	More Details
CVE-2023-34577	SQL injection vulnerability in Prestashop opartplannedpopup 1.4.11 and earlier allows remote attackers to run arbitrary SQL commands via OpartPlannedPopupModuleFrontController::prepareHook() method.	9.8	More Details
CVE-2023-43242	D-Link DIR-816 A2 v1.10CNB05 was discovered to contain a stack overflow via parameter removeRuleList in form2IPQoSTcDel.	9.8	More Details

CVE Number	Description	Base Score	Reference
CVE-2023-43241	D-Link DIR-823G v1.0.2B05 was discovered to contain a stack overflow via parameter TXPower and GuardInt in SetWLanRadioSecurity.	9.8	More Details
CVE-2023-43338	Cesanta mjs v2.20.0 was discovered to contain a function pointer hijacking vulnerability via the function mjs_get_ptr(). This vulnerability allows attackers to execute arbitrary code via a crafted input.	9.8	More Details
CVE-2023-43469	SQL injection vulnerability in janobe Online Job Portal v.2020 allows a remote attacker to execute arbitrary code via the ForPass.php component.	9.8	More Details
CVE-2023-43238	D-Link DIR-816 A2 v1.10CNB05 was discovered to contain a stack overflow via parameter nvmacaddr in form2Dhcpip.cgi.	9.8	More Details
CVE-2023-43470	SQL injection vulnerability in janobe Online Voting System v.1.0 allows a remote attacker to execute arbitrary code via the checklogin.php component.	9.8	More Details
CVE-2023-41294	The DP module has a service hijacking vulnerability.Successful exploitation of this vulnerability may affect some Super Device services.	9.8	More Details
CVE-2023-41297	Vulnerability of defects introduced in the design process in the HiviewTunner module. Successful exploitation of this vulnerability may cause service hijacking.	9.8	More Details
CVE-2023-41419	An issue in Gevent before version 23.9.0 allows a remote attacker to escalate privileges via a crafted script to the WSGIServer component.	9.8	More Details
CVE-2022-48605	Input verification vulnerability in the fingerprint module. Successful exploitation of this vulnerability will affect confidentiality, integrity, and availability.	9.8	More Details
CVE-2023-43131	General Device Manager 2.5.2.2 is vulnerable to Buffer Overflow.	9.8	More Details
CVE-2023-32653	An out-of-bounds write vulnerability exists in the dcm_pixel_data_decode functionality of Accusoft ImageGear 20.1. A specially crafted malformed file can lead to arbitrary code execution. A victim would need to open a malicious file to trigger this vulnerability.	9.8	More Details

CVE Number	Description	Base Score	Reference
CVE-2023-35002	A heap-based buffer overflow vulnerability exists in the pictwread functionality of Accusoft ImageGear 20.1. A specially crafted malformed file can lead to arbitrary code execution. An attacker can provide a malicious file to trigger this vulnerability.	9.8	More Details
CVE-2023-39453	A use-after-free vulnerability exists in the tif_parse_sub_IFD functionality of Accusoft ImageGear 20.1. A specially crafted malformed file can lead to arbitrary code execution. An attacker can deliver this file to trigger this vulnerability.	9.8	More Details
CVE-2023-40163	An out-of-bounds write vulnerability exists in the allocate_buffer_for_jpeg_decoding functionality of Accusoft ImageGear 20.1. A specially crafted malformed file can lead to memory corruption. An attacker can provide a malicious file to trigger this vulnerability.	9.8	More Details
CVE-2023-43141	TOTOLINK A3700R V9.1.2u.6134_B20201202 and N600R V5.3c.5137 are vulnerable to Incorrect Access Control.	9.8	More Details
CVE-2023-4490	The WP Job Portal WordPress plugin before 2.0.6 does not sanitise and escape a parameter before using it in a SQL statement, leading to a SQL injection exploitable by unauthenticated users	9.8	More Details
CVE-2023-4521	The Import XML and RSS Feeds WordPress plugin before 2.1.5 contains a web shell, allowing unauthenticated attackers to perform RCE. The plugin/vendor was not compromised and the files are the result of running a PoC for a previously reported issue (https://wpscan.com/vulnerability/d4220025-2272-4d5f-9703-4b2ac4a51c42) and not deleting the created files when releasing the new version.	9.8	More Details
CVE-2023-39640	UpLight cookiebanner before 1.5.1 was discovered to contain a SQL injection vulnerability via the component Hook::getHookModuleExecList().	9.8	More Details
CVE-2023-43239	D-Link DIR-816 A2 v1.10CNB05 was discovered to contain a stack overflow via parameter flag_5G in showMACfilterMAC.	9.8	More Details
CVE-2023-43457	An issue in Service Provider Management System v.1.0 allows a remote attacker to gain privileges via the ID parameter in the /php-spms/admin/?page=user/ endpoint.	9.8	More Details
CVE-2023-43237	D-Link DIR-816 A2 v1.10CNB05 was discovered to contain a stack overflow via parameter macCloneMac in setMAC.	9.8	More Details

CVE Number	Description	Base Score	Reference
CVE-2023-40619	phpPgAdmin 7.14.4 and earlier is vulnerable to deserialization of untrusted data which may lead to remote code execution because user-controlled data is directly passed to the PHP 'unserialize()' function in multiple places. An example is the functionality to manage tables in 'tables.php' where the 'ma[]' POST parameter is deserialized.	9.8	More Details
CVE-2019-19450	paraparser in ReportLab before 3.5.31 allows remote code execution because start_unichar in paraparser.py evaluates untrusted user input in a unichar element in a crafted XML document with '<unichar code="' followed by arbitrary Python code, a similar issue to CVE-2019-17626.	9.8	More Details
CVE-2023-43196	D-Link DI-7200GV2.E1 v21.04.09E1 was discovered to contain a stack overflow via the zn_jb parameter in the arp_sys.asp function.	9.8	More Details
CVE-2023-43197	D-Link device DI-7200GV2.E1 v21.04.09E1 was discovered to contain a stack overflow via the fn parameter in the tgfile.asp function.	9.8	More Details
CVE-2023-43198	D-Link device DI-7200GV2.E1 v21.04.09E1 was discovered to contain a stack overflow via the popupId parameter in the H5/hi_block.asp function.	9.8	More Details
CVE-2023-43199	D-Link device DI-7200GV2.E1 v21.04.09E1 was discovered to contain a stack overflow via the prev parameter in the H5/login.cgi function.	9.8	More Details
CVE-2023-43200	D-Link device DI-7200GV2.E1 v21.04.09E1 was discovered to contain a stack overflow via the id parameter in the yyxz.data function.	9.8	More Details
CVE-2023-43201	D-Link device DI-7200GV2.E1 v21.04.09E1 was discovered to contain a stack overflow via the hi_up parameter in the qos_ext.asp function.	9.8	More Details
CVE-2023-43202	D-LINK DWL-6610 FW_v_4.3.0.8B003C was discovered to contain a command injection vulnerability in the function pcap_download_handler. This vulnerability allows attackers to execute arbitrary commands via the update.device.packet-capture.tftp-file-name parameter.	9.8	More Details
CVE-2023-43203	D-LINK DWL-6610 FW_v_4.3.0.8B003C was discovered to contain a stack overflow vulnerability in the function update_users.	9.8	More Details

CVE Number	Description	Base Score	Reference
CVE-2023-43204	D-LINK DWL-6610 FW_v_4.3.0.8B003C was discovered to contain a command injection vulnerability in the function sub_2EF50. This vulnerability allows attackers to execute arbitrary commands via the manual-time-string parameter.	9.8	More Details
CVE-2023-43206	D-LINK DWL-6610 FW_v_4.3.0.8B003C was discovered to contain a command injection vulnerability in the function web_cert_download_handler. This vulnerability allows attackers to execute arbitrary commands via the certDownload parameter.	9.8	More Details
CVE-2023-43207	D-LINK DWL-6610 FW_v_4.3.0.8B003C was discovered to contain a command injection vulnerability in the function config_upload_handler. This vulnerability allows attackers to execute arbitrary commands via the configRestore parameter.	9.8	More Details
CVE-2023-42464	A Type Confusion vulnerability was found in the Spotlight RPC functions in afpd in Netatalk 3.1.x before 3.1.17. When parsing Spotlight RPC packets, one encoded data structure is a key-value style dictionary where the keys are character strings, and the values can be any of the supported types in the underlying protocol. Due to a lack of type checking in callers of the dalloc_value_for_key() function, which returns the object associated with a key, a malicious actor may be able to fully control the value of the pointer and theoretically achieve Remote Code Execution on the host. This issue is similar to CVE-2023-34967.	9.8	More Details
CVE-2023-5074	Use of a static key to protect a JWT token used in user authentication can allow an for an authentication bypass in D-Link D-View 8 v2.0.1.28	9.8	More Details
CVE-2023-2262	A buffer overflow vulnerability exists in the Rockwell Automation select 1756-EN* communication devices. If exploited, a threat actor could potentially leverage this vulnerability to perform a remote code execution. To exploit this vulnerability, a threat actor would have to send a maliciously crafted CIP request to device.	9.8	More Details
CVE-2023-43371	Hoteldruid v3.0.5 was discovered to contain a SQL injection vulnerability via the numcaselle parameter at /hoteldruid/creaprezzi.php.	9.8	More Details
CVE-2023-34575	SQL injection vulnerability in PrestaShop opartsavecart through 2.0.7 allows remote attackers to run arbitrary SQL commands via OpartSaveCartDefaultModuleFrontController::initContent() and OpartSaveCartDefaultModuleFrontController::displayAjaxSendCartByEmail() methods.	9.8	More Details

CVE Number	Description	Base Score	Reference
CVE-2023-43236	D-Link DIR-816 A2 v1.10CNB05 was discovered to contain a stack overflow via parameter statuscheckpppoeuser in dir_setWanWifi.	9.8	More Details
CVE-2023-43235	D-Link DIR-823G v1.0.2B05 was discovered to contain a stack overflow via parameter StartTime and EndTime in SetWifiDownSettings.	9.8	More Details
CVE-2023-4291	Frauscher Sensortechnik GmbH FDS101 for FAdC/FAdCi v1.4.24 and all previous versions are vulnerable to a remote code execution (RCE) vulnerability via manipulated parameters of the web interface without authentication. This could lead to a full compromise of the FDS101 device.	9.8	More Details
CVE-2015-5467	web\ViewAction in Yii (aka Yii2) 2.x before 2.0.5 allows attackers to execute any local .php file via a relative path in the view parameeter.	9.8	More Details
CVE-2023-43135	There is an unauthorized access vulnerability in TP-LINK ER5120G 4.0 2.0.0 Build 210817 Rel.80868n, which allows attackers to obtain sensitive information of the device without authentication, obtain user tokens, and ultimately log in to the device backend management.	9.8	More Details
CVE-2023-39675	SimpleImportProduct Prestashop Module v6.2.9 was discovered to contain a SQL injection vulnerability via the key parameter at send.php.	9.8	More Details
CVE-2023-43373	Hoteldruid v3.0.5 was discovered to contain a SQL injection vulnerability via the n_utente_agg parameter at /hoteldruid/interconnessioni.php.	9.8	More Details
CVE-2023-36109	Buffer Overflow vulnerability in JerryScript version 3.0, allows remote attackers to execute arbitrary code via ecma_stringbuilder_append_raw component at /jerry-core/ecma/base/ecma-helpers-string.c.	9.8	More Details
CVE-2023-42322	Insecure Permissions vulnerability in icmsdev iCMS v.7.0.16 allows a remote attacker to obtain sensitive information.	9.8	More Details
CVE-2023-43134	There is an unauthorized access vulnerability in Netis 360RAC1200 v1.3.4517, which allows attackers to obtain sensitive information of the device without authentication, obtain user tokens, and ultimately log in to the device backend management.	9.8	More Details
CVE-2023-43375	Hoteldruid v3.0.5 was discovered to contain multiple SQL injection vulnerabilities at /hoteldruid/clienti.php via the annonascita, annoscaddoc, giornonascita, giornoscaddoc, lingua_cli, mesenascita, and mesescaddoc parameters.	9.8	More Details

CVE Number	Description	Base Score	Reference
CVE-2023-43374	Hoteldruid v3.0.5 was discovered to contain a SQL injection vulnerability via the id_utente_log parameter at /hoteldruid/personalizza.php.	9.8	More Details
CVE-2023-38888	Cross Site Scripting vulnerability in Dolibarr ERP CRM v.17.0.1 and before allows a remote attacker to obtain sensitive information and execute arbitrary code via the REST API module, related to analyseVarsForSqlAndScriptsInjection and testSqlAndScriptInject.	9.6	More Details
CVE-2023-4088	Incorrect Default Permissions vulnerability in Mitsubishi Electric Corporation multiple FA engineering software products allows a malicious local attacker to execute a malicious code, resulting in information disclosure, tampering with and deletion, or a denial-of-service (DoS) condition, if the product is installed in a folder other than the default installation folder.	9.3	More Details
CVE-2023-41296	Vulnerability of missing authorization in the kernel module. Successful exploitation of this vulnerability may affect integrity and confidentiality.	9.1	More Details
CVE-2023-39407	The Watchkit has a risk of unauthorized file access.Successful exploitation of this vulnerability may affect confidentiality and integrity.	9.1	More Details
CVE-2023-0118	An arbitrary code execution flaw was found in Foreman. This flaw allows an admin user to bypass safe mode in templates and execute arbitrary code on the underlying operating system.	9.1	More Details
CVE-2023-43644	Sing-box is an open source proxy system. Affected versions are subject to an authentication bypass when specially crafted requests are sent to sing-box. This affects all SOCKS5 inbounds with user authentication and an attacker may be able to bypass authentication. Users are advised to update to sing-box 1.4.4 or to 1.5.0-rc.4. Users unable to update should not expose the SOCKS5 inbound to insecure environments.	9.1	More Details
CVE-2023-43632	As noted in the “VTPM.md” file in the eve documentation, “VTPM is a server listening on port 8877 in EVE, exposing limited functionality of the TPM to the clients. VTPM allows clients to execute tpm2-tools binaries from a list of hardcoded options” The communication with this server is done using protobuf, and the data is comprised of 2 parts: 1. Header 2. Data When a connection is made, the server is waiting for 4 bytes of data, which will be the header, and these 4 bytes would be parsed as uint32 size of the actual data to come. Then, in the function “handleRequest” this size is then used in order to allocate a payload on the stack for the incoming data. As this payload is allocated on the stack, this will allow overflowing the stack size allocated for the relevant process with freely controlled data. * An attacker can crash the system. * An attacker can gain control over the system, specifically on the “vtpm_server” process which has very high privileges.	9.0	More Details

OTHER VULNERABILITIES

CVE Number	Description	Base Score	Reference
CVE-2023-43496	Jenkins 2.423 and earlier, LTS 2.414.1 and earlier creates a temporary file in the system temporary directory with the default permissions for newly created files when installing a plugin from a URL, potentially allowing attackers with access to the system temporary directory to replace the file before it is installed in Jenkins, potentially resulting in arbitrary code execution.	8.8	More Details
CVE-2023-43382	Directory Traversal vulnerability in itechyou dreamer CMS v.4.1.3 allows a remote attacker to execute arbitrary code via the themePath in the uploaded template function.	8.8	More Details
CVE-2023-0829	Plesk 17.0 through 18.0.31 version, is vulnerable to a Cross-Site Scripting. A malicious subscription owner (either a customer or an additional user), can fully compromise the server if an administrator visits a certain page in Plesk related to the malicious subscription.	8.8	More Details
CVE-2023-43478	fake_upload.cgi on the Telstra Smart Modem Gen 2 (Arcadyan LH1000), firmware versions < 0.18.15r, allows unauthenticated attackers to upload firmware images and configuration backups, which could allow them to alter the firmware or the configuration on the device, ultimately leading to code execution as root.	8.8	More Details
CVE-2023-43630	PCR14 is not in the list of PCRs that seal/unseal the “vault” key, but due to the change that was implemented in commit “7638364bc0acf8b5c481b5ce5fea11ad44ad7fd4”, fixing this issue alone would not solve the problem of the config partition not being measured correctly. Also, the “vault” key is sealed/unsealed with SHA1 PCRs instead of SHA256. This issue was somewhat mitigated due to all of the PCR extend functions updating both the values of SHA256 and SHA1 for a given PCR ID. However, due to the change that was implemented in commit “7638364bc0acf8b5c481b5ce5fea11ad44ad7fd4”, this is no longer the case for PCR14, as the code in “measurefs.go” explicitly updates only the SHA256 instance of PCR14, which means that even if PCR14 were to be added to the list of PCRs sealing/unsealing the “vault” key, changes to the config partition would still not be measured. An attacker could modify the config partition without triggering the measured boot, this could result in the attacker gaining full control over the device with full access to the contents of the encrypted “vault”	8.8	More Details

CVE Number	Description	Base Score	Reference
CVE-2023-43635	Vault Key Sealed With SHA1 PCRs The measured boot solution implemented in EVE OS leans on a PCR locking mechanism. Different parts of the system update different PCR values in the TPM, resulting in a unique value for each PCR entry. These PCRs are then used in order to seal/unseal a key from the TPM which is used to encrypt/decrypt the “vault” directory. This “vault” directory is the most sensitive point in the system and as such, its content should be protected. This mechanism is noted in Zededa’s documentation as the “measured boot” mechanism, designed to protect said “vault”. The code that’s responsible for generating and fetching the key from the TPM assumes that SHA256 PCRs are used in order to seal/unseal the key, and as such their presence is being checked. The issue here is that the key is not sealed using SHA256 PCRs, but using SHA1 PCRs. This leads to several issues: • Machines that have their SHA256 PCRs enabled but SHA1 PCRs disabled, as well as not sealing their keys at all, meaning the “vault” is not protected from an attacker. • SHA1 is considered insecure and reduces the complexity level required to unseal the key in machines which have their SHA1 PCRs enabled. An attacker can very easily retrieve the contents of the “vault”, which will effectively render the “measured boot” mechanism meaningless.	8.8	More Details
CVE-2023-43636	In EVE OS, the “measured boot” mechanism prevents a compromised device from accessing the encrypted data located in the vault. As per the “measured boot” design, the PCR values calculated at different stages of the boot process will change if any of their respective parts are changed. This includes, among other things, the configuration of the bios, grub, the kernel cmdline, initrd, and more. However, this mechanism does not validate the entire rootfs, so an attacker can edit the filesystem and gain control over the system. As the default filesystem used by EVE OS is squashfs, this is somewhat harder than an ext4, which is easily changeable. This will not stop an attacker, as an attacker can repackage the squashfs with their changes in it and replace the partition altogether. This can also be done directly on the device, as the “003-storage-init” container contains the “mksquashfs” and “unsquashfs” binaries (with the corresponding libs). An attacker can gain full control over the device without changing the PCR values, thus not triggering the “measured boot” mechanism, and having full access to the vault. Note: This issue was partially fixed in these commits (after disclosure to Zededa), where the config partition measurement was added to PCR13: • aa3501d6c57206ced222c33aea15a9169d629141 • 5fef4d92e75838cc78010edaed5247dfbdae1889. This issue was made viable in version 9.0.0 when the calculation was moved to PCR14 but it was not included in the measured boot.	8.8	More Details

CVE Number	Description	Base Score	Reference
CVE-2023-42660	In Progress MOVEit Transfer versions released before 2021.1.8 (13.1.8), 2022.0.8 (14.0.8), 2022.1.9 (14.1.9), 2023.0.6 (15.0.6), a SQL injection vulnerability has been identified in the MOVEit Transfer machine interface that could allow an authenticated attacker to gain unauthorized access to the MOVEit Transfer database. An attacker could submit a crafted payload to the MOVEit Transfer machine interface which could result in modification and disclosure of MOVEit database content.	8.8	More Details
CVE-2023-43500	A cross-site request forgery (CSRF) vulnerability in Jenkins Build Failure Analyzer Plugin 2.4.1 and earlier allows attackers to connect to an attacker-specified hostname and port using attacker-specified username and password.	8.8	More Details
CVE-2023-38346	An issue was discovered in Wind River VxWorks 6.9 and 7. The function ``tarExtract`` implements TAR file extraction and thereby also processes files within an archive that have relative or absolute file paths. A developer using the "tarExtract" function may expect that the function will strip leading slashes from absolute paths or stop processing when encountering relative paths that are outside of the extraction path, unless otherwise forced. This could lead to unexpected and undocumented behavior, which in general could result in a directory traversal, and associated unexpected behavior.	8.8	More Details
CVE-2023-42331	A file upload vulnerability in EliteCMS v1.01 allows a remote attacker to execute arbitrary code via the manage_uploads.php component.	8.8	More Details
CVE-2023-42335	Unrestricted File Upload vulnerability in Fl3xx Dispatch 2.10.37 and fl3xx Crew 2.10.37 allows a remote attacker to execute arbitrary code via the add attachment function in the New Expense component.	8.8	More Details
CVE-2023-43137	TPLINK TL-ER5120G 4.0 2.0.0 Build 210817 Rel.80868n has a command injection vulnerability, when an attacker adds ACL rules after authentication, and the rule name parameter has injection points.	8.8	More Details
CVE-2023-43138	TPLINK TL-ER5120G 4.0 2.0.0 Build 210817 Rel.80868n has a command injection vulnerability, when an attacker adds NAPT rules after authentication, and the rule name has an injection point.	8.8	More Details
CVE-2023-42321	Cross Site Request Forgery (CSRF) vulnerability in icmsdev iCMSv.7.0.16 allows a remote attacker to execute arbitrary code via the user.admincp.php, members.admincp.php, and group.admincp.php files.	8.8	More Details

CVE Number	Description	Base Score	Reference
CVE-2015-8371	Composer before 2016-02-10 allows cache poisoning from other projects built on the same host. This results in attacker-controlled code entering a server-side build process. The issue occurs because of the way that dist packages are cached. The cache key is derived from the package name, the dist type, and certain other data from the package repository (which may simply be a commit hash, and thus can be found by an attacker). Versions through 1.0.0-alpha11 are affected, and 1.0.0 is unaffected.	8.8	More Details
CVE-2023-43631	On boot, the Pillar eve container checks for the existence and content of “/config/authorized_keys”. If the file is present, and contains a supported public key, the container will go on to open port 22 and enable sshd with the given keys as the authorized keys for root login. An attacker could easily add their own keys and gain full control over the system without triggering the “measured boot” mechanism implemented by EVE OS, and without marking the device as “UUD” (“Unknown Update Detected”). This is because the “/config” partition is not protected by “measured boot”, it is mutable, and it is not encrypted in any way. An attacker can gain full control over the device without changing the PCR values, thus not triggering the “measured boot” mechanism, and having full access to the vault. Note: This issue was partially fixed in these commits (after disclosure to Zededa), where the config partition measurement was added to PCR13: • aa3501d6c57206ced222c33aea15a9169d629141 • 5fef4d92e75838cc78010edaed5247dfbdae1889. This issue was made viable in version 9.0.0 when the calculation was moved to PCR14 but it was not included in the measured boot.	8.8	More Details

CVE Number	Description	Base Score	Reference
CVE-2023-43633	On boot, the Pillar eve container checks for the existence and content of “/config/GlobalConfig/global.json”. If the file exists, it overrides the existing configuration on the device on boot. This allows an attacker to change the system’s configuration, which also includes some debug functions. This could be used to unlock the ssh with custom “authorized_keys” via the “debug.enable.ssh” key, similar to the “authorized_keys” finding that was noted before. Other usages include unlocking the usb to enable the keyboard via the “debug.enable.usb” key, allowing VNC access via the “app.allow.vnc” key, and more. An attacker could easily enable these debug functionalities without triggering the “measured boot” mechanism implemented by EVE OS, and without marking the device as “UUD” (“Unknown Update Detected”). This is because the “/config” partition is not protected by “measured boot”, it is mutable and it is not encrypted in any way. An attacker can gain full control over the device without changing the PCR values, thereby not triggering the “measured boot” mechanism, and having full access to the vault. Note: This issue was partially fixed in these commits (after disclosure to Zededa), where the config partition measurement was added to PCR13: • aa3501d6c57206ced222c33aea15a9169d629141 • 5fef4d92e75838cc78010edaed5247dfbdae1889. This issue was made viable in version 9.0.0 when the calculation was moved to PCR14 but it was not included in the measured boot.	8.8	More Details
CVE-2023-43634	When sealing/unsealing the “vault” key, a list of PCRs is used, which defines which PCRs are used. In a previous project, CYMOTIVE found that the configuration is not protected by the secure boot, and in response Zededa implemented measurements on the config partition that was mapped to PCR 13. In that process, PCR 13 was added to the list of PCRs that seal/unseal the key. In commit “56e589749c6ff58ded862d39535d43253b249acf”, the config partition measurement moved from PCR 13 to PCR 14, but PCR 14 was not added to the list of PCRs that seal/unseal the key. This change makes the measurement of PCR 14 effectively redundant as it would not affect the sealing/unsealing of the key. An attacker could modify the config partition without triggering the measured boot, this could result in the attacker gaining full control over the device with full access to the contents of the encrypted “vault”	8.8	More Details
CVE-2023-23362	An OS command injection vulnerability has been reported to affect QNAP operating systems. If exploited, the vulnerability allows remote authenticated users to execute commands via susceptible QNAP devices. We have already fixed the vulnerability in the following versions: QTS 5.0.1.2376 build 20230421 and later QTS 4.5.4.2374 build 20230416 and later QuTS hero h5.0.1.2376 build 20230421 and later QuTS hero h4.5.4.2374 build 20230417 and later QuTScloud c5.0.1.2374 and later	8.8	More Details

CVE Number	Description	Base Score	Reference
CVE-2023-41993	The issue was addressed with improved checks. This issue is fixed in macOS Sonoma 14. Processing web content may lead to arbitrary code execution. Apple is aware of a report that this issue may have been actively exploited against versions of iOS before iOS 16.7.	8.8	More Details
CVE-2023-3547	The All in One B2B for WooCommerce WordPress plugin through 1.0.3 does not properly check nonce values in several actions, allowing an attacker to perform CSRF attacks.	8.8	More Details
CVE-2023-36319	File Upload vulnerability in Openupload Stable v.0.4.3 allows a remote attacker to execute arbitrary code via the action parameter of the compress-inc.php file.	8.8	More Details
CVE-2023-38887	File Upload vulnerability in Dolibarr ERP CRM v.17.0.1 and before allows a remote attacker to execute arbitrary code and obtain sensitive information via the extension filtering and renaming functions.	8.8	More Details
CVE-2023-25528	NVIDIA DGX H100 baseboard management controller (BMC) contains a vulnerability in a web server plugin, where an unauthenticated attacker may cause a stack overflow by sending a specially crafted network packet. A successful exploit of this vulnerability may lead to arbitrary code execution, denial of service, information disclosure, and data tampering.	8.8	More Details
CVE-2023-43278	A Cross-Site Request Forgery (CSRF) in admin_manager.php of Seacms up to v12.8 allows attackers to arbitrarily add an admin account.	8.8	More Details
CVE-2023-4258	In Bluetooth mesh implementation If provisionee has a public key that is sent OOB then during provisioning it can be sent back and will be accepted by provisionee.	8.6	More Details
CVE-2023-37410	IBM Personal Communications 14.05, 14.06, and 15.0.0 could allow a local user to escalate their privileges to the SYSTEM user due to overly permissive access controls. IBM X-Force ID: 260138.	8.4	More Details
CVE-2023-25533	NVIDIA DGX H100 BMC contains a vulnerability in the web UI, where an attacker may cause improper input validation. A successful exploit of this vulnerability may lead to information disclosure, code execution, and escalation of privileges.	8.3	More Details

CVE Number	Description	Base Score	Reference
CVE-2023-40581	yt-dlp is a youtube-dl fork with additional features and fixes. yt-dlp allows the user to provide shell command lines to be executed at various stages in its download steps through the `--exec` flag. This flag allows output template expansion in its argument, so that metadata values may be used in the shell commands. The metadata fields can be combined with the `%q` conversion, which is intended to quote/escape these values so they can be safely passed to the shell. However, the escaping used for `cmd` (the shell used by Python's `subprocess` on Windows) does not properly escape special characters, which can allow for remote code execution if `--exec` is used directly with maliciously crafted remote data. This vulnerability only impacts `yt-dlp` on Windows, and the vulnerability is present regardless of whether `yt-dlp` is run from `cmd` or from `PowerShell`. Support for output template expansion in `--exec`, along with this vulnerable behavior, was added to `yt-dlp` in version 2021.04.11. yt-dlp version 2023.09.24 fixes this issue by properly escaping each special character. `\n` will be replaced by `\r` as no way of escaping it has been found. It is recommended to upgrade yt-dlp to version 2023.09.24 as soon as possible. Also, always be careful when using --exec, because while this specific vulnerability has been patched, using unvalidated input in shell commands is inherently dangerous. For Windows users who are not able to upgrade: 1. Avoid using any output template expansion in --exec other than {} (filepath). 2. If expansion in --exec is needed, verify the fields you are using do not contain ",	or &. 3. Instead of using --exec, write the info json and load the fields from it instead.	8.3	More Details
CVE-2023-31009	NVIDIA DGX H100 BMC contains a vulnerability in the REST service, where an attacker may cause improper input validation. A successful exploit of this vulnerability may lead to code execution, denial of service, escalation of privileges, and information disclosure.	8.3	More Details
CVE-2023-42798	AutomataCI is a template git repository equipped with a native built-in semi-autonomous CI tools. An issue in versions 1.4.1 and below can let a release job reset the git root repository to the first commit. Version 1.5.0 has a patch for this issue. As a workaround, make sure the `PROJECT_PATH_RELEASE` (e.g. `releases/`) directory is manually and actually `git cloned` properly, making it a different git repostiory from the root git repository.	8.2	More Details
CVE-2023-43497	In Jenkins 2.423 and earlier, LTS 2.414.1 and earlier, processing file uploads using the Stapler web framework creates temporary files in the default system temporary directory with the default permissions for newly created files, potentially allowing attackers with access to the Jenkins controller file system to read and write the files before they are used.	8.1	More Details

CVE Number	Description	Base Score	Reference
CVE-2023-23364	A buffer copy without checking size of input vulnerability has been reported to affect QNAP operating systems. If exploited, the vulnerability possibly allows remote users to execute code via unspecified vectors. We have already fixed the vulnerability in the following versions: Multimedia Console 2.1.1 (2023/03/29) and later Multimedia Console 1.4.7 (2023/03/20) and later	8.1	More Details
CVE-2023-23567	A heap-based buffer overflow vulnerability exists in the CreateDIBfromPict functionality of Accusoft ImageGear 20.1. A specially crafted file can lead to arbitrary code execution. An attacker can provide a malicious file to trigger this vulnerability.	8.1	More Details
CVE-2023-23363	A buffer copy without checking size of input vulnerability has been reported to affect QNAP operating system. If exploited, the vulnerability possibly allows remote users to execute code via unspecified vectors. We have already fixed the vulnerability in the following versions: QTS 4.3.6.2441 build 20230621 and later QTS 4.3.3.2420 build 20230621 and later QTS 4.2.6 build 20230621 and later QTS 4.3.4.2451 build 20230621 and later	8.1	More Details
CVE-2023-32284	An out-of-bounds write vulnerability exists in the tiff_planar_adobe functionality of Accusoft ImageGear 20.1. A specially crafted malformed file can lead to memory corruption. An attacker can provide a malicious file to trigger this vulnerability.	8.1	More Details
CVE-2023-4853	A flaw was found in Quarkus where HTTP security policies are not sanitizing certain character permutations correctly when accepting requests, resulting in incorrect evaluation of permissions. This issue could allow an attacker to bypass the security policy altogether, resulting in unauthorized endpoint access and possibly a denial of service.	8.1	More Details
CVE-2022-4137	A reflected cross-site scripting (XSS) vulnerability was found in the 'oob' OAuth endpoint due to incorrect null-byte handling. This issue allows a malicious link to insert an arbitrary URI into a Keycloak error page. This flaw requires a user or administrator to interact with a link in order to be vulnerable. This may compromise user details, allowing it to be changed or collected by an attacker.	8.1	More Details
CVE-2023-43498	In Jenkins 2.423 and earlier, LTS 2.414.1 and earlier, processing file uploads using MultipartFormDataParser creates temporary files in the default system temporary directory with the default permissions for newly created files, potentially allowing attackers with access to the Jenkins controller file system to read and write the files before they are used.	8.1	More Details
CVE-2023-41484	An issue in cimg.eu Cimg Library v2.9.3 allows an attacker to obtain sensitive information via a crafted JPEG file.	8.1	More Details

CVE Number	Description	Base Score	Reference
CVE-2023-0462	An arbitrary code execution flaw was found in Foreman. This issue may allow an admin user to execute arbitrary code on the underlying operating system by setting global parameters with a YAML payload.	8.0	More Details
CVE-2023-25530	NVIDIA DGX H100 BMC contains a vulnerability in the KVM service, where an attacker may cause improper input validation. A successful exploit of this vulnerability may lead to code execution, denial of service, escalation of privileges, and information disclosure.	8.0	More Details
CVE-2022-3874	A command injection flaw was found in foreman. This flaw allows an authenticated user with admin privileges on the foreman instance to transpile commands through CoreOS and Fedora CoreOS configurations in templates, possibly resulting in arbitrary command execution on the underlying operating system.	8.0	More Details
CVE-2023-41031	Command injection in homemng.htm in Juplink RX4-1500 versions V1.0.2, V1.0.3, V1.0.4, and V1.0.5 allows remote authenticated attackers to execute commands via specially crafted requests to the vulnerable endpoint.	8.0	More Details
CVE-2023-41029	Command injection vulnerability in the homemng.htm endpoint in Juplink RX4-1500 Wifi router firmware versions V1.0.2, V1.0.3, V1.0.4, and V1.0.5 allows authenticated remote attackers to execute commands as root via specially crafted HTTP requests to the vulnerable endpoint.	8.0	More Details
CVE-2023-41027	Credential disclosure in the '/webs/userpasswd.htm' endpoint in Juplink RX4-1500 Wifi router firmware versions V1.0.4 and V1.0.5 allows an authenticated attacker to leak the password for the administrative account via requests to the vulnerable endpoint.	8.0	More Details
CVE-2023-0625	Docker Desktop before 4.12.0 is vulnerable to RCE via a crafted extension description or changelog. This issue affects Docker Desktop: before 4.12.0.	8.0	More Details
CVE-2023-25529	NVIDIA DGX H100 BMC and DGX A100 BMC contains a vulnerability in the host KVM daemon, where an unauthenticated attacker may cause a leak of another user’s session token by observing timing discrepancies between server responses. A successful exploit of this vulnerability may lead to information disclosure, escalation of privileges, and data tampering.	8.0	More Details
CVE-2023-1260	An authentication bypass vulnerability was discovered in kube-apiserver. This issue could allow a remote, authenticated attacker who has been given permissions "update, patch" the "pods/ephemeralcontainers" subresource beyond what the default is. They would then need to create a new pod or patch one that they already have access to. This might allow evasion of SCC admission restrictions, thereby gaining control of a privileged pod.	8.0	More Details

CVE Number	Description	Base Score	Reference
CVE-2022-4039	A flaw was found in Red Hat Single Sign-On for OpenShift container images, which are configured with an unsecured management interface enabled. This flaw allows an attacker to use this interface to deploy malicious code and access and modify potentially sensitive information in the app server configuration.	8.0	More Details
CVE-2023-5166	Docker Desktop before 4.23.0 allows Access Token theft via a crafted extension icon URL. This issue affects Docker Desktop: before 4.23.0.	8.0	More Details
CVE-2023-0626	Docker Desktop before 4.12.0 is vulnerable to RCE via query parameters in message-box route. This issue affects Docker Desktop: before 4.12.0.	8.0	More Details
CVE-2023-41375	Use after free vulnerability exists in Kostac PLC Programming Software Version 1.6.11.0. Arbitrary code may be executed by having a user open a specially crafted project file which was saved using Kostac PLC Programming Software Version 1.6.9.0 and earlier because the issue exists in parsing of KPP project files. The vendor states that Kostac PLC Programming Software Version 1.6.10.0 or later implements the function which prevents a project file alteration. Therefore, to mitigate the impact of these vulnerabilities, a project file which was saved using Kostac PLC Programming Software Version 1.6.9.0 and earlier needs to be saved again using Kostac PLC Programming Software Version 1.6.10.0 or later.	7.8	More Details
CVE-2023-41992	The issue was addressed with improved checks. This issue is fixed in macOS Monterey 12.7, iOS 16.7 and iPadOS 16.7, macOS Ventura 13.6. A local attacker may be able to elevate their privileges. Apple is aware of a report that this issue may have been actively exploited against versions of iOS before iOS 16.7.	7.8	More Details
CVE-2023-43619	An issue was discovered in Croc through 9.6.5. A sender may send dangerous new files to a receiver, such as executable content or a .ssh/authorized_keys file.	7.8	More Details
CVE-2023-43620	An issue was discovered in Croc through 9.6.5. A sender may place ANSI or CSI escape sequences in a filename to attack the terminal device of a receiver.	7.8	More Details
CVE-2023-5068	Delta Electronics DIAScreen may write past the end of an allocated buffer while parsing a specially crafted input file. This could allow an attacker to execute code in the context of the current process.	7.8	More Details

CVE Number	Description	Base Score	Reference
CVE-2023-34319	The fix for XSA-423 added logic to Linux'es netback driver to deal with a frontend splitting a packet in a way such that not all of the headers would come in one piece. Unfortunately the logic introduced there didn't account for the extreme case of the entire packet being split into as many pieces as permitted by the protocol, yet still being smaller than the area that's specially dealt with to keep all (possible) headers together. Such an unusual packet would therefore trigger a buffer overrun in the driver.	7.8	More Details
CVE-2023-41374	Double free issue exists in Kostac PLC Programming Software Version 1.6.11.0 and earlier. Arbitrary code may be executed by having a user open a specially crafted project file which was saved using Kostac PLC Programming Software Version 1.6.9.0 and earlier because the issue exists in parsing of KPP project files. The vendor states that Kostac PLC Programming Software Version 1.6.10.0 or later implements the function which prevents a project file alteration. Therefore, to mitigate the impact of these vulnerabilities, a project file which was saved using Kostac PLC Programming Software Version 1.6.9.0 and earlier needs to be saved again using Kostac PLC Programming Software Version 1.6.10.0 or later.	7.8	More Details
CVE-2023-43766	Certain WithSecure products allow Local privilege escalation via the lhz archive unpack handler. This affects WithSecure Client Security 15, WithSecure Server Security 15, WithSecure Email and Server Security 15, WithSecure Elements Endpoint Protection 17 and later, WithSecure Client Security for Mac 15, WithSecure Elements Endpoint Protection for Mac 17 and later, Linux Security 64 12.0 , Linux Protection 12.0, and WithSecure Atlant (formerly F-Secure Atlant) 1.0.35-1.	7.8	More Details
CVE-2023-41902	An XPC misconfiguration vulnerability in CoreCode MacUpdater before 2.3.8, and 3.x before 3.1.2, allows attackers to escalate privileges by crafting malicious .pkg files.	7.8	More Details
CVE-2023-25527	NVIDIA DGX H100 BMC contains a vulnerability in the host KVM daemon, where an authenticated local attacker may cause corruption of kernel memory. A successful exploit of this vulnerability may lead to arbitrary kernel code execution, denial of service, escalation of privileges, information disclosure, and data tampering.	7.8	More Details
CVE-2022-4318	A vulnerability was found in cri-o. This issue allows the addition of arbitrary lines into /etc/passwd by use of a specially crafted environment variable.	7.8	More Details

CVE Number	Description	Base Score	Reference
CVE-2023-43637	Due to the implementation of "deriveVaultKey", prior to version 7.10, the generated vault key would always have the last 16 bytes predetermined to be "arfoobarfoobarfo". This issue happens because "deriveVaultKey" calls "retrieveCloudKey" (which will always return "foobarfoobarfoobarfoobarfoobarfo" as the key), and then merges the 32byte randomly generated key with this key (by takeing 16bytes from each, see "mergeKeys"). This makes the key a lot weaker. This issue does not persist in devices that were initialized on/after version 7.10, but devices that were initialized before that and updated to a newer version still have this issue. Roll an update that enforces the full 32bytes key usage.	7.8	More Details
CVE-2023-25531	NVIDIA DGX H100 BMC contains a vulnerability in IPMI, where an attacker may cause insufficient protection of credentials. A successful exploit of this vulnerability may lead to code execution, denial of service, information disclosure, and escalation of privileges.	7.6	More Details
CVE-2023-4760	In Eclipse RAP versions from 3.0.0 up to and including 3.25.0, Remote Code Execution is possible on Windows when using the FileUpload component. The reason for this is a not completely secure extraction of the file name in the FileUploadProcessor.stripFileName(String name) method. As soon as this finds a / in the path, everything before it is removed, but potentially \ (backslashes) coming further back are kept. For example, a file name such as /..\..\webapps\shell.war can be used to upload a file to a Tomcat server under Windows, which is then saved as ..\..\webapps\shell.war in its webapps directory and can then be executed.	7.6	More Details
CVE-2023-4152	Frauscher Sensortechnik GmbH FDS101 for FAdC/FAdCi v1.4.24 and all previous versions are vulnerable to a path traversal vulnerability of the web interface by a crafted URL without authentication. This enables an remote attacker to read all files on the filesystem of the FDS101 device.	7.5	More Details
CVE-2023-43784	Plesk Onyx 17.8.11 has accessKeyId and secretAccessKey fields that are related to an Amazon AWS Firehose component. NOTE: the vendor's position is that there is no security threat.	7.5	More Details
CVE-2023-42280	mee-admin 1.5 is vulnerable to Directory Traversal. The download method in the CommonFileController.java file does not verify the incoming data, resulting in arbitrary file reading.	7.5	More Details
CVE-2023-38907	An issue in TPLink Smart Bulb Tapo series L530 before 1.2.4, L510E before 1.1.0, L630 before 1.0.4, P100 before 1.5.0, and Tapo Application 2.8.14 allows a remote attacker to replay old messages encrypted with a still valid session key.	7.5	More Details

CVE Number	Description	Base Score	Reference
CVE-2023-40183	DataEase is an open source data visualization and analysis tool. Prior to version 1.18.11, DataEase has a vulnerability that allows an attacker to to obtain user cookies. The program only uses the `ImageIO.read()` method to determine whether the file is an image file or not. There is no whitelisting restriction on file suffixes. This allows the attacker to synthesize the attack code into an image for uploading and change the file extension to html. The attacker may steal user cookies by accessing links. The vulnerability has been fixed in v1.18.11. There are no known workarounds.	7.5	More Details
CVE-2023-31716	FUXA <= 1.1.12 has a Local File Inclusion vulnerability via file=fuxa.log	7.5	More Details
CVE-2023-43274	Phpjabbers PHP Shopping Cart 4.2 is vulnerable to SQL Injection via the id parameter.	7.5	More Details
CVE-2023-31717	A SQL Injection attack in FUXA <= 1.1.12 allows exfiltration of confidential information from the database.	7.5	More Details
CVE-2023-42805	quinn-proto is a state machine for the QUIC transport protocol. Prior to versions 0.9.5 and 0.10.5, receiving unknown QUIC frames in a QUIC packet could result in a panic. The problem has been fixed in 0.9.5 and 0.10.5 maintenance releases.	7.5	More Details
CVE-2023-42457	plone.rest allows users to use HTTP verbs such as GET, POST, PUT, DELETE, etc. in Plone. Starting in the 2.x branch and prior to versions 2.0.1 and 3.0.1, when the `++api++` traverser is accidentally used multiple times in a url, handling it takes increasingly longer, making the server less responsive. Patches are available in `plone.rest` 2.0.1 and 3.0.1. Series 1.x is not affected. As a workaround, one may redirect `/++api++/++api++` to `/++api++` in one's frontend web server (nginx, Apache).	7.5	More Details
CVE-2023-39677	MyPrestaModules Prestashop Module v6.2.9 and UpdateProducts Prestashop Module v3.6.9 were discovered to contain a PHPInfo information disclosure vulnerability via send.php.	7.5	More Details
CVE-2023-31718	FUXA <= 1.1.12 is vulnerable to Local via Inclusion via /api/download.	7.5	More Details
CVE-2023-43783	Cadence through 0.9.2 2023-08-21 uses an Insecure /tmp/cadence-wineasio.reg Temporary File. The filename is used even if it has been created by a local adversary before Cadence started. The adversary can leverage this to create or overwrite files via a symlink attack. In some kernel configurations, code injection into the Wine registry is possible.	7.5	More Details

CVE Number	Description	Base Score	Reference
CVE-2023-37279	Faktory is a language-agnostic persistent background job server. Prior to version 1.8.0, the Faktory web dashboard can suffer from denial of service by a crafted malicious url query param `days`. The vulnerability is related to how the backend reads the `days` URL query parameter in the Faktory web dashboard. The value is used directly without any checks to create a string slice. If a very large value is provided, the backend server ends up using a significant amount of memory and causing it to crash. Version 1.8.0 fixes this issue.	7.5	More Details
CVE-2023-43760	Certain WithSecure products allow Denial of Service via a fuzzed PE32 file. This affects WithSecure Client Security 15, WithSecure Server Security 15, WithSecure Email and Server Security 15, WithSecure Elements Endpoint Protection 17 and later, WithSecure Client Security for Mac 15, WithSecure Elements Endpoint Protection for Mac 17 and later, Linux Security 64 12.0 , Linux Protection 12.0, and WithSecure Atlant (formerly F-Secure Atlant) 1.0.35-1.	7.5	More Details
CVE-2023-43761	Certain WithSecure products allow Denial of Service (infinite loop). This affects WithSecure Client Security 15, WithSecure Server Security 15, WithSecure Email and Server Security 15, WithSecure Elements Endpoint Protection 17 and later, WithSecure Client Security for Mac 15, WithSecure Elements Endpoint Protection for Mac 17 and later, Linux Security 64 12.0 , Linux Protection 12.0, and WithSecure Atlant (formerly F-Secure Atlant) 1.0.35-1.	7.5	More Details
CVE-2023-43765	Certain WithSecure products allow Denial of Service in the aeelf component. This affects WithSecure Client Security 15, WithSecure Server Security 15, WithSecure Email and Server Security 15, WithSecure Elements Endpoint Protection 17 and later, WithSecure Client Security for Mac 15, WithSecure Elements Endpoint Protection for Mac 17 and later, Linux Security 64 12.0 , Linux Protection 12.0, and WithSecure Atlant (formerly F-Secure Atlant) 1.0.35-1.	7.5	More Details
CVE-2023-43669	The Tungstenite crate before 0.20.1 for Rust allows remote attackers to cause a denial of service (minutes of CPU consumption) via an excessive length of an HTTP header in a client handshake. The length affects both how many times a parse is attempted (e.g., thousands of times) and the average amount of data for each parse attempt (e.g., millions of bytes).	7.5	More Details
CVE-2023-25525	NVIDIA Cumulus Linux contains a vulnerability in forwarding where a VxLAN-encapsulated IPv6 packet received on an SVI interface with DMAC/DIPv6 set to the link-local address of the SVI interface may be incorrectly forwarded. A successful exploit may lead to information disclosure.	7.5	More Details

CVE Number	Description	Base Score	Reference
CVE-2023-43767	Certain WithSecure products allow Denial of Service via the aepack archive unpack handler. This affects WithSecure Client Security 15, WithSecure Server Security 15, WithSecure Email and Server Security 15, WithSecure Elements Endpoint Protection 17 and later, WithSecure Client Security for Mac 15, WithSecure Elements Endpoint Protection for Mac 17 and later, Linux Security 64 12.0 , Linux Protection 12.0, and WithSecure Atlant (formerly F-Secure Atlant) 1.0.35-1.	7.5	More Details
CVE-2023-42261	Mobile Security Framework (MobSF) <=v3.7.8 Beta is vulnerable to Insecure Permissions. NOTE: the vendor's position is that authentication is intentionally not implemented because the product is not intended for an untrusted network environment. Use cases requiring authentication could, for example, use a reverse proxy server.	7.5	More Details
CVE-2023-43642	snappy-java is a Java port of the snappy, a fast C++ compresser/decompresser developed by Google. The SnappyInputStream was found to be vulnerable to Denial of Service (DoS) attacks when decompressing data with a too large chunk size. Due to missing upper bound check on chunk length, an unrecoverable fatal error can occur. All versions of snappy-java including the latest released version 1.1.10.3 are vulnerable to this issue. A fix has been introduced in commit `9f8c3cf74` which will be included in the 1.1.10.4 release. Users are advised to upgrade. Users unable to upgrade should only accept compressed data from trusted sources.	7.5	More Details
CVE-2023-41293	Data security classification vulnerability in the DDMP module. Successful exploitation of this vulnerability may affect confidentiality.	7.5	More Details
CVE-2023-5042	Sensitive information disclosure due to insecure folder permissions. The following products are affected: Acronis Cyber Protect Home Office (Windows) before build 40713.	7.5	More Details
CVE-2022-47562	Vulnerability in the RCPbind service running on UDP port (111), allowing a remote attacker to create a denial of service (DoS) condition.	7.5	More Details

CVE Number	Description	Base Score	Reference
CVE-2023-3341	The code that processes control channel messages sent to `named` calls certain functions recursively during packet parsing. Recursion depth is only limited by the maximum accepted packet size; depending on the environment, this may cause the packet-parsing code to run out of available stack memory, causing `named` to terminate unexpectedly. Since each incoming control channel message is fully parsed before its contents are authenticated, exploiting this flaw does not require the attacker to hold a valid RNDC key; only network access to the control channel's configured TCP port is necessary. This issue affects BIND 9 versions 9.2.0 through 9.16.43, 9.18.0 through 9.18.18, 9.19.0 through 9.19.16, 9.9.3-S1 through 9.16.43-S1, and 9.18.0-S1 through 9.18.18-S1.	7.5	More Details
CVE-2023-4236	A flaw in the networking code handling DNS-over-TLS queries may cause `named` to terminate unexpectedly due to an assertion failure. This happens when internal data structures are incorrectly reused under significant DNS-over-TLS query load. This issue affects BIND 9 versions 9.18.0 through 9.18.18 and 9.18.11-S1 through 9.18.18-S1.	7.5	More Details
CVE-2022-4244	A flaw was found in codeplex-codehaus. A directory traversal attack (also known as path traversal) aims to access files and directories stored outside the intended folder. By manipulating files with "dot-dot-slash (../)" sequences and their variations or by using absolute file paths, it may be possible to access arbitrary files and directories stored on the file system, including application source code, configuration, and other critical system files.	7.5	More Details
CVE-2023-41303	Command injection vulnerability in the distributed file system module. Successful exploitation of this vulnerability may cause variables in the sock structure to be modified.	7.5	More Details
CVE-2023-42147	An issue in CloudExplorer Lite 1.3.1 allows an attacker to obtain sensitive information via the login key component.	7.5	More Details
CVE-2023-41302	Redirection permission verification vulnerability in the home screen module. Successful exploitation of this vulnerability may cause features to perform abnormally.	7.5	More Details
CVE-2023-41301	Vulnerability of unauthorized API access in the PMS module. Successful exploitation of this vulnerability may cause features to perform abnormally.	7.5	More Details
CVE-2023-41300	Vulnerability of parameters not being strictly verified in the PMS module. Successful exploitation of this vulnerability may cause the system to restart.	7.5	More Details

CVE Number	Description	Base Score	Reference
CVE-2023-38343	An XXE (XML external entity injection) vulnerability exists in the CSEP component of Ivanti Endpoint Manager before 2022 SU4. External entity references are enabled in the XML parser configuration. Exploitation of this vulnerability can lead to file disclosure or Server Side Request Forgery.	7.5	More Details
CVE-2023-41299	DoS vulnerability in the PMS module. Successful exploitation of this vulnerability may cause the system to restart.	7.5	More Details
CVE-2023-41298	Vulnerability of permission control in the window module. Successful exploitation of this vulnerability may affect confidentiality.	7.5	More Details
CVE-2023-39409	DoS vulnerability in the PMS module. Successful exploitation of this vulnerability may cause the system to restart.	7.5	More Details
CVE-2023-39408	DoS vulnerability in the PMS module. Successful exploitation of this vulnerability may cause the system to restart.	7.5	More Details
CVE-2023-5156	A flaw was found in the GNU C Library. A recent fix for CVE-2023-4806 introduced the potential for a memory leak, which may result in an application crash.	7.5	More Details
CVE-2023-42821	The package `github.com/gomarkdown/markdown` is a Go library for parsing Markdown text and rendering as HTML. Prior to pseudoversion `0.0.0-20230922105210-14b16010c2ee`, which corresponds with commit `14b16010c2ee7ff33a940a541d993bd043a88940`, parsing malformed markdown input with parser that uses parser.Mmark extension could result in out-of-bounds read vulnerability. To exploit the vulnerability, parser needs to have `parser.Mmark` extension set. The panic occurs inside the `citation.go` file on the line 69 when the parser tries to access the element past its length. This can result in a denial of service. Commit `14b16010c2ee7ff33a940a541d993bd043a88940`/pseudoversion `0.0.0-20230922105210-14b16010c2ee` contains a patch for this issue.	7.5	More Details
CVE-2022-3596	An information leak was found in OpenStack's undercloud. This flaw allows unauthenticated, remote attackers to inspect sensitive data after discovering the IP address of the undercloud, possibly leading to compromising private information, including administrator access credentials.	7.5	More Details

CVE Number	Description	Base Score	Reference
CVE-2023-1625	An information leak was discovered in OpenStack heat. This issue could allow a remote, authenticated attacker to use the 'stack show' command to reveal parameters which are supposed to remain hidden. This has a low impact to the confidentiality, integrity, and availability of the system.	7.4	More Details
CVE-2023-3550	Mediawiki v1.40.0 does not validate namespaces used in XML files. Therefore, if the instance administrator allows XML file uploads, a remote attacker with a low-privileged user account can use this exploit to become an administrator by sending a malicious link to the instance administrator.	7.3	More Details
CVE-2022-47561	The web application stores credentials in clear text in the "admin.xml" file, which can be accessed without logging into the website, which could allow an attacker to obtain credentials related to all users, including admin users, in clear text, and use them to subsequently execute malicious actions.	7.3	More Details
CVE-2023-31008	NVIDIA DGX H100 BMC contains a vulnerability in IPMI, where an attacker may cause improper input validation. A successful exploit of this vulnerability may lead to code execution, denial of services, escalation of privileges, and information disclosure.	7.3	More Details
CVE-2023-4238	The Prevent files / folders access WordPress plugin before 2.5.2 does not validate files to be uploaded, which could allow attackers to upload arbitrary files such as PHP on the server.	7.2	More Details
CVE-2023-4300	The Import XML and RSS Feeds WordPress plugin before 2.1.4 does not filter file extensions for uploaded files, allowing an attacker to upload a malicious PHP file, leading to Remote Code Execution.	7.2	More Details
CVE-2023-3664	The FileOrganizer WordPress plugin through 1.0.2 does not restrict functionality on multisite instances, allowing site admins to gain full control over the server.	7.2	More Details
CVE-2023-40043	In Progress MOVEit Transfer versions released before 2021.1.8 (13.1.8), 2022.0.8 (14.0.8), 2022.1.9 (14.1.9), 2023.0.6 (15.0.6), a SQL injection vulnerability has been identified in the MOVEit Transfer web interface that could allow a MOVEit system administrator account to gain unauthorized access to the MOVEit Transfer database. A MOVEit system administrator could submit a crafted payload to the MOVEit Transfer web interface which could result in modification and disclosure of MOVEit database content.	7.2	More Details
CVE-2023-0633	In Docker Desktop on Windows before 4.12.0 an argument injection to installer may result in local privilege escalation (LPE).This issue affects Docker Desktop: before 4.12.0.	7.2	More Details
CVE-2023-38886	An issue in Dolibarr ERP CRM v.17.0.1 and before allows a remote privileged attacker to execute arbitrary code via a crafted command/script.	7.2	More Details

CVE Number	Description	Base Score	Reference
CVE-2023-41868	Unauth. Reflected Cross-Site Scripting (XSS) vulnerability in Ram Ratan Maurya, Codestag StagTools plugin <= 2.3.7 versions.	7.1	More Details
CVE-2023-41871	Unauth. Reflected Cross-Site Scripting (XSS) vulnerability in Poll Maker Team Poll Maker plugin <= 4.7.0 versions.	7.1	More Details
CVE-2023-41867	Unauth. Reflected Cross-Site Scripting (XSS) vulnerability in AcyMailing Newsletter Team AcyMailing plugin <= 8.6.2 versions.	7.1	More Details
CVE-2023-41872	Unauth. Reflected Cross-Site Scripting (XSS) vulnerability in Xtemos WoodMart plugin <= 7.2.4 versions.	7.1	More Details
CVE-2023-41874	Unauth. Reflected Cross-Site Scripting (XSS) vulnerability in Tyche Softwares Order Delivery Date for WooCommerce plugin <= 3.20.0 versions.	7.1	More Details
CVE-2023-5165	Docker Desktop before 4.23.0 allows an unprivileged user to bypass Enhanced Container Isolation (ECI) restrictions via the debug shell which remains accessible for a short time window after launching Docker Desktop. The affected functionality is available for Docker Business customers only and assumes an environment where users are not granted local root or Administrator privileges. This issue has been fixed in Docker Desktop 4.23.0. Affected Docker Desktop versions: from 4.13.0 before 4.23.0.	7.1	More Details
CVE-2023-41863	Unauth. Stored Cross-Site Scripting (XSS) vulnerability in Pepro Dev. Group PeproDev CF7 Database plugin <= 1.7.0 versions.	7.1	More Details
CVE-2023-4259	Two potential buffer overflow vulnerabilities at the following locations in the Zephyr eS-WiFi driver source code.	7.1	More Details
CVE-2023-42753	An array indexing vulnerability was found in the netfilter subsystem of the Linux kernel. A missing macro could lead to a miscalculation of the `h->nets` array offset, providing attackers with the primitive to arbitrarily increment/decrement a memory buffer out-of-bound. This issue may allow a local user to crash the system or potentially escalate their privileges on the system.	7.0	More Details

CVE Number	Description	Base Score	Reference
CVE-2023-32614	A heap-based buffer overflow vulnerability exists in the create_png_object functionality of Accusoft ImageGear 20.1. A specially crafted malformed file can lead to memory corruption. An attacker can provide a malicious file to trigger this vulnerability.	7.0	More Details
CVE-2023-4504	Due to failure in validating the length provided by an attacker-crafted PPD PostScript document, CUPS and libppd are susceptible to a heap-based buffer overflow and possibly code execution. This issue has been fixed in CUPS version 2.4.7, released in September of 2023.	7.0	More Details
CVE-2023-31010	NVIDIA DGX H100 BMC contains a vulnerability in IPMI, where an attacker may cause improper input validation. A successful exploit of this vulnerability may lead to escalation of privileges, information disclosure, and denial of service.	6.8	More Details
CVE-2022-3916	A flaw was found in the offline_access scope in Keycloak. This issue would affect users of shared computers more (especially if cookies are not cleared), due to a lack of root session validation, and the reuse of session ids across root and user authentication sessions. This enables an attacker to resolve a user session attached to a previously authenticated user; when utilizing the refresh token, they will be issued a token for the original user.	6.8	More Details
CVE-2023-40930	An issue in the directory /system/bin/blkid of Skyworth v3.0 allows attackers to perform a directory traversal via mounting the Udisk to /mnt/.	6.8	More Details
CVE-2023-43477	The ping_from parameter of ping_tracerte.cgi in the web UI of Telstra Smart Modem Gen 2 (Arcadyan LH1000), firmware versions < 0.18.15r, was not properly sanitized before being used in a system call, which could allow an authenticated attacker to achieve command injection as root on the device.	6.8	More Details
CVE-2023-0627	Docker Desktop 4.11.x allows --no-windows-containers flag bypass via IPC response spoofing which may lead to Local Privilege Escalation (LPE).This issue affects Docker Desktop: 4.11.X.	6.7	More Details
CVE-2023-31015	NVIDIA DGX H100 BMC contains a vulnerability in the REST service where a host user may cause as improper authentication issue. A successful exploit of this vulnerability may lead to escalation of privileges, information disclosure, code execution, and denial of service.	6.6	More Details
CVE-2023-1633	A credentials leak flaw was found in OpenStack Barbican. This flaw allows a local authenticated attacker to read the configuration file, gaining access to sensitive credentials.	6.6	More Details

CVE Number	Description	Base Score	Reference
CVE-2023-39052	An information leak in Earthgarden_waiting 13.6.1 allows attackers to obtain the channel access token and send crafted messages.	6.5	More Details
CVE-2023-42334	An Indirect Object Reference (IDOR) in Fl3xx Dispatch 2.10.37 and fl3xx Crew 2.10.37 allows a remote attacker to escalate privileges via the user parameter.	6.5	More Details
CVE-2023-39044	An information leak in ajino-Shiretoko Line v13.6.1 allows attackers to obtain the channel access token and send crafted messages.	6.5	More Details
CVE-2023-39041	An information leak in KUKURUDELI Line v13.6.1 allows attackers to obtain the channel access token and send crafted messages.	6.5	More Details
CVE-2023-43256	A path traversal in Gladys Assistant v4.26.1 and below allows authenticated attackers to extract sensitive files in the host machine by exploiting a non-sanitized user input.	6.5	More Details
CVE-2023-39045	An information leak in kokoroe_members card Line 13.6.1 allows attackers to obtain the channel access token and send crafted messages.	6.5	More Details
CVE-2023-43640	TaxonWorks is a web-based workbench designed for taxonomists and biodiversity scientists. Prior to version 0.34.0, a SQL injection vulnerability was found in TaxonWorks that allows authenticated attackers to extract arbitrary data from the TaxonWorks database (including the users table). This issue may lead to information disclosure. Version 0.34.0 contains a fix for the issue.	6.5	More Details
CVE-2023-38344	An issue was discovered in Ivanti Endpoint Manager before 2022 SU4. A file disclosure vulnerability exists in the GetFileContents SOAP action exposed via /landesk/managementsuite/core/core.secure/OsdScript.asmx. The application does not sufficiently restrict user-supplied paths, allowing for an authenticated attacker to read arbitrary files from a remote system, including the private key used to authenticate to agents for remote access.	6.5	More Details
CVE-2023-43501	A missing permission check in Jenkins Build Failure Analyzer Plugin 2.4.1 and earlier allows attackers with Overall/Read permission to connect to an attacker-specified hostname and port using attacker-specified username and password.	6.5	More Details
CVE-2023-5104	Improper Input Validation in GitHub repository nocodb/nocodb prior to 0.96.0.	6.5	More Details

CVE Number	Description	Base Score	Reference
CVE-2023-5158	A flaw was found in vringh_kiov_advance in drivers/vhost/vringh.c in the host side of a virtio ring in the Linux Kernel. This issue may result in a denial of service from guest to host via zero length descriptor.	6.5	More Details
CVE-2023-25526	NVIDIA Cumulus Linux contains a vulnerability in neighmgrd and nlmanager where an attacker on an adjacent network may cause an uncaught exception by injecting a crafted packet. A successful exploit may lead to denial of service.	6.5	More Details
CVE-2023-25532	NVIDIA DGX H100 BMC contains a vulnerability in IPMI, where an attacker may cause insufficient protection of credentials. A successful exploit of this vulnerability may lead to information disclosure.	6.5	More Details
CVE-2023-43132	szvone vmqphp <=1.13 is vulnerable to SQL Injection. Unauthorized remote users can use sql injection attacks to obtain the hash of the administrator password.	6.5	More Details
CVE-2023-42806	Hydra is the layer-two scalability solution for Cardano. Prior to version 0.13.0, not signing and verifying `$\mathsf{cid}$` allows an attacker (which must be a participant of this head) to use a snapshot from an old head instance with the same participants to close the head or contest the state with it. This can lead to an incorrect distribution of value (= value extraction attack; hard, but possible) or prevent the head to finalize because the value available is not consistent with the closed utxo state (= denial of service; easy). A patch is planned for version 0.13.0. As a workaround, rotate keys between heads so not to re-use keys and not result in the same multi-signature participants.	6.5	More Details
CVE-2022-45447	M4 PDF plugin for Prestashop sites, in its 3.2.3 version and before, is vulnerable to a directory traversal vulnerability. The “f” parameter is not properly checked in the resource /m4pdf/pdf.php, returning any file given its relative path. An attacker that exploits this vulnerability could download /etc/passwd from the server if the file exists.	6.5	More Details
CVE-2023-5063	The Widget Responsive for Youtube plugin for WordPress is vulnerable to Stored Cross-Site Scripting via 'youtube' shortcode in versions up to, and including, 1.6.1 due to insufficient input sanitization and output escaping on user supplied attributes. This makes it possible for authenticated attackers with contributor-level and above permissions to inject arbitrary web scripts in pages that will execute whenever a user accesses an injected page.	6.4	More Details

CVE Number	Description	Base Score	Reference
CVE-2023-5125	The Contact Form by FormGet plugin for WordPress is vulnerable to Stored Cross-Site Scripting via 'formget' shortcode in versions up to, and including, 5.5.5 due to insufficient input sanitization and output escaping on user supplied attributes. This makes it possible for authenticated attackers with contributor-level and above permissions to inject arbitrary web scripts in pages that will execute whenever a user accesses an injected page.	6.4	More Details
CVE-2022-1438	A flaw was found in Keycloak. Under specific circumstances, HTML entities are not sanitized during user impersonation, resulting in a Cross-site scripting (XSS) vulnerability.	6.4	More Details
CVE-2023-4774	The WP-Matomo Integration (WP-Piwik) plugin for WordPress is vulnerable to Stored Cross-Site Scripting via the 'wp-piwik' shortcode in versions up to, and including, 1.0.28 due to insufficient input sanitization and output escaping on user supplied attributes. This makes it possible for authenticated attackers with contributor-level and above permissions to inject arbitrary web scripts in pages that will execute whenever a user accesses an injected page.	6.4	More Details
CVE-2023-4716	The Media Library Assistant plugin for WordPress is vulnerable to Stored Cross-Site Scripting via the 'mla_gallery' shortcode in versions up to, and including, 3.10 due to insufficient input sanitization and output escaping on user supplied attributes. This makes it possible for authenticated attackers with contributor-level and above permissions to inject arbitrary web scripts in pages that will execute whenever a user accesses an injected page.	6.4	More Details
CVE-2023-5062	The WordPress Charts plugin for WordPress is vulnerable to Stored Cross-Site Scripting via 'wp_charts' shortcode in versions up to, and including, 0.7.0 due to insufficient input sanitization and output escaping on user supplied attributes. This makes it possible for authenticated attackers with contributor-level and above permissions to inject arbitrary web scripts in pages that will execute whenever a user accesses an injected page.	6.4	More Details
CVE-2023-5149	** UNSUPPORTED WHEN ASSIGNED ** A vulnerability was found in D-Link DAR-7000 up to 20151231. It has been rated as critical. This issue affects some unknown processing of the file /useratte/userattestation.php. The manipulation of the argument web_img leads to unrestricted upload. The attack may be initiated remotely. The exploit has been disclosed to the public and may be used. The identifier VDB-240245 was assigned to this vulnerability. NOTE: This vulnerability only affects products that are no longer supported by the maintainer. NOTE: Vendor was contacted early and confirmed immediately that the product is end-of-life. It should be retired and replaced.	6.3	More Details

CVE Number	Description	Base Score	Reference
CVE-2023-5150	** UNSUPPORTED WHEN ASSIGNED ** A vulnerability classified as critical has been found in D-Link DAR-7000 and DAR-8000 up to 20151231. Affected is an unknown function of the file /useratte/web.php. The manipulation of the argument file_upload leads to unrestricted upload. It is possible to launch the attack remotely. The exploit has been disclosed to the public and may be used. VDB-240246 is the identifier assigned to this vulnerability. NOTE: This vulnerability only affects products that are no longer supported by the maintainer. NOTE: Vendor was contacted early and confirmed immediately that the product is end-of-life. It should be retired and replaced.	6.3	More Details
CVE-2023-5148	** UNSUPPORTED WHEN ASSIGNED ** A vulnerability was found in D-Link DAR-7000 and DAR-8000 up to 20151231. It has been declared as critical. This vulnerability affects unknown code of the file /Tool/uploadfile.php. The manipulation of the argument file_upload leads to unrestricted upload. The attack can be initiated remotely. The exploit has been disclosed to the public and may be used. The identifier of this vulnerability is VDB-240244. NOTE: This vulnerability only affects products that are no longer supported by the maintainer. NOTE: Vendor was contacted early and confirmed immediately that the product is end-of-life. It should be retired and replaced.	6.3	More Details
CVE-2023-5147	** UNSUPPORTED WHEN ASSIGNED ** A vulnerability was found in D-Link DAR-7000 up to 20151231. It has been classified as critical. This affects an unknown part of the file /sysmanage/updateos.php. The manipulation of the argument 1_file_upload leads to unrestricted upload. It is possible to initiate the attack remotely. The exploit has been disclosed to the public and may be used. The associated identifier of this vulnerability is VDB-240243. NOTE: This vulnerability only affects products that are no longer supported by the maintainer. NOTE: Vendor was contacted early and confirmed immediately that the product is end-of-life. It should be retired and replaced.	6.3	More Details
CVE-2023-5151	** UNSUPPORTED WHEN ASSIGNED ** A vulnerability classified as critical was found in D-Link DAR-8000 up to 20151231. Affected by this vulnerability is an unknown functionality of the file /autheditpwd.php. The manipulation of the argument hid_id leads to sql injection. The attack can be launched remotely. The exploit has been disclosed to the public and may be used. The associated identifier of this vulnerability is VDB-240247. NOTE: This vulnerability only affects products that are no longer supported by the maintainer. NOTE: Vendor was contacted early and confirmed immediately that the product is end-of-life. It should be retired and replaced.	6.3	More Details

CVE Number	Description	Base Score	Reference
CVE-2023-5146	** UNSUPPORTED WHEN ASSIGNED ** A vulnerability was found in D-Link DAR-7000 and DAR-8000 up to 20151231 and classified as critical. Affected by this issue is some unknown functionality of the file /sysmanage/updatelib.php. The manipulation of the argument file_upload leads to unrestricted upload. The attack may be launched remotely. The exploit has been disclosed to the public and may be used. VDB-240242 is the identifier assigned to this vulnerability. NOTE: This vulnerability only affects products that are no longer supported by the maintainer. NOTE: Vendor was contacted early and confirmed immediately that the product is end-of-life. It should be retired and replaced.	6.3	More Details
CVE-2023-5145	** UNSUPPORTED WHEN ASSIGNED ** A vulnerability has been found in D-Link DAR-7000 up to 20151231 and classified as critical. Affected by this vulnerability is an unknown functionality of the file /sysmanage/licence.php. The manipulation of the argument file_upload leads to unrestricted upload. The attack can be launched remotely. The exploit has been disclosed to the public and may be used. The identifier VDB-240241 was assigned to this vulnerability. NOTE: This vulnerability only affects products that are no longer supported by the maintainer. NOTE: Vendor was contacted early and confirmed immediately that the product is end-of-life. It should be retired and replaced.	6.3	More Details
CVE-2023-5144	** UNSUPPORTED WHEN ASSIGNED ** A vulnerability, which was classified as critical, was found in D-Link DAR-7000 and DAR-8000 up to 20151231. Affected is an unknown function of the file /sysmanage/updateos.php. The manipulation of the argument file_upload leads to unrestricted upload. It is possible to launch the attack remotely. The exploit has been disclosed to the public and may be used. The identifier of this vulnerability is VDB-240240. NOTE: This vulnerability only affects products that are no longer supported by the maintainer. NOTE: Vendor was contacted early and confirmed that the product is end-of-life. It should be retired and replaced.	6.3	More Details
CVE-2023-5152	** UNSUPPORTED WHEN ASSIGNED ** A vulnerability, which was classified as critical, has been found in D-Link DAR-7000 and DAR-8000 up to 20151231. Affected by this issue is some unknown functionality of the file /importexport.php. The manipulation of the argument sql leads to sql injection. The attack may be launched remotely. The exploit has been disclosed to the public and may be used. The identifier of this vulnerability is VDB-240248. NOTE: This vulnerability only affects products that are no longer supported by the maintainer. NOTE: Vendor was contacted early and confirmed immediately that the product is end-of-life. It should be retired and replaced.	6.3	More Details

CVE Number	Description	Base Score	Reference
CVE-2023-5143	** UNSUPPORTED WHEN ASSIGNED ** A vulnerability, which was classified as critical, has been found in D-Link DAR-7000 up to 20151231. This issue affects some unknown processing of the file /log/webmailattach.php. The manipulation of the argument table_name leads to an unknown weakness. The attack may be initiated remotely. The exploit has been disclosed to the public and may be used. The associated identifier of this vulnerability is VDB-240239. NOTE: This vulnerability only affects products that are no longer supported by the maintainer. NOTE: Vendor was contacted early and confirmed immediately that the product is end-of-life. It should be retired and replaced.	6.3	More Details
CVE-2023-5153	** UNSUPPORTED WHEN ASSIGNED ** A vulnerability, which was classified as critical, was found in D-Link DAR-8000 up to 20151231. This affects an unknown part of the file /Tool/querysql.php. The manipulation leads to sql injection. It is possible to initiate the attack remotely. The exploit has been disclosed to the public and may be used. The identifier VDB-240249 was assigned to this vulnerability. NOTE: This vulnerability only affects products that are no longer supported by the maintainer. NOTE: Vendor was contacted early and confirmed immediately that the product is end-of-life. It should be retired and replaced.	6.3	More Details
CVE-2023-5154	** UNSUPPORTED WHEN ASSIGNED ** A vulnerability has been found in D-Link DAR-8000 up to 20151231 and classified as critical. This vulnerability affects unknown code of the file /sysmanage/changelogo.php. The manipulation of the argument file_upload leads to unrestricted upload. The attack can be initiated remotely. The exploit has been disclosed to the public and may be used. VDB-240250 is the identifier assigned to this vulnerability. NOTE: This vulnerability only affects products that are no longer supported by the maintainer. NOTE: Vendor was contacted early and confirmed immediately that the product is end-of-life. It should be retired and replaced.	6.3	More Details
CVE-2023-42807	Frappe LMS is an open source learning management system. In versions 1.0.0 and prior, on the People Page of LMS, there was an SQL Injection vulnerability. The issue has been fixed in the `main` branch. Users won't face this issue if they are using the latest main branch of the app.	6.3	More Details
CVE-2023-42812	Galaxy is an open-source platform for FAIR data analysis. Prior to version 22.05, Galaxy is vulnerable to server-side request forgery, which allows a malicious to issue arbitrary HTTP/HTTPS requests from the application server to internal hosts and read their responses. Version 22.05 contains a patch for this issue.	6.3	More Details
CVE-2023-42426	Cross-site scripting (XSS) vulnerability in Froala Froala Editor v.4.1.1 allows remote attackers to execute arbitrary code via the 'Insert link' parameter in the 'Insert Image' component.	6.1	More Details

CVE Number	Description	Base Score	Reference
CVE-2023-31012	NVIDIA DGX H100 BMC contains a vulnerability in the REST service where an attacker may cause improper input validation. A successful exploit of this vulnerability may lead to escalation of privileges and information disclosure.	6.1	More Details
CVE-2023-43319	Cross Site Scripting (XSS) vulnerability in the Sign-In page of IceWarp WebClient 10.3.5 allows attackers to execute arbitrary web scripts or HTML via a crafted payload injected into the username parameter.	6.1	More Details
CVE-2023-43763	Certain WithSecure products allow XSS via an unvalidated parameter in the endpoint. This affects WithSecure Policy Manager 15 on Windows and Linux.	6.1	More Details
CVE-2023-43339	Cross-Site Scripting (XSS) vulnerability in cmsmadesimple v.2.2.18 allows a local attacker to execute arbitrary code via a crafted payload injected into the Database Name, DataBase User or Database Port components.	6.1	More Details
CVE-2023-38876	A reflected cross-site scripting (XSS) vulnerability in msaad1999's PHP-Login-System 2.0.1 allows remote attackers to execute arbitrary JavaScript in the web browser of a user, by including a malicious payload into the 'selector' parameter in '/reset-password'.	6.1	More Details
CVE-2023-38875	A reflected cross-site scripting (XSS) vulnerability in msaad1999's PHP-Login-System 2.0.1 allows remote attackers to execute arbitrary JavaScript in the web browser of a user, by including a malicious payload into the 'validator' parameter in '/reset-password'.	6.1	More Details
CVE-2023-42656	In Progress MOVEit Transfer versions released before 2021.1.8 (13.1.8), 2022.0.8 (14.0.8), 2022.1.9 (14.1.9), 2023.0.6 (15.0.6), a reflected cross-site scripting (XSS) vulnerability has been identified in MOVEit Transfer's web interface. An attacker could craft a malicious payload targeting MOVEit Transfer users during the package composition procedure. If a MOVEit user interacts with the crafted payload, the attacker would be able to execute malicious JavaScript within the context of the victims browser.	6.1	More Details
CVE-2023-43326	A reflected cross-site scripting (XSS) vulnerability exisits in multiple url of mooSocial v3.1.8 allows attackers to steal user's session cookies and impersonate their account via a crafted URL.	6.1	More Details
CVE-2023-43770	Roundcube before 1.4.14, 1.5.x before 1.5.4, and 1.6.x before 1.6.3 allows XSS via text/plain e-mail messages with crafted links because of program/lib/Roundcube/rcube_string_replacer.php behavior.	6.1	More Details

CVE Number	Description	Base Score	Reference
CVE-2023-40618	A reflected cross-site scripting (XSS) vulnerability in OpenKnowledgeMaps Head Start versions 4, 5, 6, 7 as well as Visual Project Explorer 1.0, allows remote attackers to execute arbitrary JavaScript in the web browser of a user, by including a malicious payload into the 'service' parameter in 'headstart_snapshot.php'.	6.1	More Details
CVE-2023-31013	NVIDIA DGX H100 BMC contains a vulnerability in the REST service, where an attacker may cause improper input validation. A successful exploit of this vulnerability may lead to escalation of privileges and information disclosure.	6.1	More Details
CVE-2023-4476	The Locatoraid Store Locator WordPress plugin before 3.9.24 does not sanitise and escape the lpr-search parameter before outputting it back in the page, leading to a Reflected Cross-Site Scripting which could be used against high privilege users such as admin.	6.1	More Details
CVE-2023-4549	The DoLogin Security WordPress plugin before 3.7 does not properly sanitize IP addresses coming from the X-Forwarded-For header, which can be used by attackers to conduct Stored XSS attacks via WordPress' login form.	6.1	More Details
CVE-2018-5478	Contao 3.x before 3.5.32 allows XSS via the unsubscribe module in the frontend newsletter extension.	6.1	More Details
CVE-2023-43325	A reflected cross-site scripting (XSS) vulnerability in the data[redirect_url] parameter of mooSocial v3.1.8 allows attackers to steal user's session cookies and impersonate their account via a crafted URL.	6.1	More Details
CVE-2023-4148	The Ditty WordPress plugin before 3.1.25 does not sanitise and escape some parameters and generated URLs before outputting them back in attributes, leading to Reflected Cross-Site Scripting which could be used against high privilege users such as admin.	6.1	More Details
CVE-2023-5002	A flaw was found in pgAdmin. This issue occurs when the pgAdmin server HTTP API validates the path a user selects to external PostgreSQL utilities such as pg_dump and pg_restore. Versions of pgAdmin prior to 7.6 failed to properly control the server code executed on this API, allowing an authenticated user to run arbitrary commands on the server.	6.0	More Details
CVE-2023-1636	A vulnerability was found in OpenStack Barbican containers. This vulnerability is only applicable to deployments that utilize an all-in-one configuration. Barbican containers share the same CGROUP, USER, and NET namespace with the host system and other OpenStack services. If any service is compromised, it could gain access to the data transmitted to and from Barbican.	6.0	More Details

CVE Number	Description	Base Score	Reference
CVE-2023-41949	Auth. (admin+) Cross-Site Scripting (XSS) vulnerability in Avirtum iFolders plugin <= 1.5.0 versions.	5.9	More Details
CVE-2023-41948	Auth. (admin+) Stored Cross-Site Scripting (XSS) vulnerability in Christoph Rado Cookie Notice & Consent plugin <= 1.6.0 versions.	5.9	More Details
CVE-2023-39252	Dell SCG Policy Manager 5.16.00.14 contains a broken cryptographic algorithm vulnerability. A remote unauthenticated attacker may potentially exploit this vulnerability by performing MitM attacks and let attackers obtain sensitive information.	5.9	More Details
CVE-2023-25534	NVIDIA DGX H100 BMC contains a vulnerability in IPMI, where an attacker may cause improper input validation. A successful exploit of this vulnerability may lead to code execution, denial of service, escalation of privileges, information disclosure, and data tampering.	5.7	More Details
CVE-2023-4892	Teedy v1.11 has a vulnerability in its text editor that allows events to be executed in HTML tags that an attacker could manipulate. Thanks to this, it is possible to execute malicious JavaScript in the webapp.	5.7	More Details
CVE-2022-47560	The lack of web request control on ekorCCP and ekorRCI devices allows a potential attacker to create custom requests to execute malicious actions when a user is logged in.	5.7	More Details
CVE-2023-28393	A stack-based buffer overflow vulnerability exists in the tif_processing_dng_channel_count functionality of Accusoft ImageGear 20.1. A specially crafted malformed file can lead to memory corruption. An attacker can provide a malicious file to trigger this vulnerability.	5.6	More Details
CVE-2023-22644	A user can reverse engineer the JWT token (JSON Web Token) used in authentication for Manager and API access, forging a valid NeuVector Token to perform malicious activity in NeuVector. This can lead to an RCE.	5.5	More Details
CVE-2023-43090	A vulnerability was found in GNOME Shell. GNOME Shell's lock screen allows an unauthenticated local user to view windows of the locked desktop session by using keyboard shortcuts to unlock the restricted functionality of the screenshot tool.	5.5	More Details
CVE-2020-24089	An issue was discovered in ImfHpRegFilter.sys in IOBit Malware Fighter version 8.0.2, allows local attackers to cause a denial of service (DoS).	5.5	More Details

CVE Number	Description	Base Score	Reference
CVE-2023-43782	Cadence through 0.9.2 2023-08-21 uses an Insecure /tmp/.cadence-aloop-daemon.x Temporary File. The file is used even if it has been created by a local adversary before Cadence started. The adversary can then delete the file, disrupting Cadence.	5.5	More Details
CVE-2023-43771	In nqptp-message-handlers.c in nqptp before 1.2.3, crafted packets received on the control port could crash the program.	5.5	More Details
CVE-2023-22024	In the Unbreakable Enterprise Kernel (UEK), the RDS module in UEK has two setsockopt(2) options, RDS_CONN_RESET and RDS6_CONN_RESET, that are not re-entrant. A malicious local user with CAP_NET_ADMIN can use this to crash the kernel. CVSS 3.1 Base Score 5.5 (Availability impacts). CVSS Vector: (CVSS:3.1/AV:L/AC:L/PR:L/UI:N/S:U/C:N/I:N/A:H).	5.5	More Details
CVE-2023-20597	Improper initialization of variables in the DXE driver may allow a privileged user to leak sensitive information via local access.	5.5	More Details
CVE-2023-41991	A certificate validation issue was addressed. This issue is fixed in macOS Ventura 13.6, iOS 16.7 and iPadOS 16.7. A malicious app may be able to bypass signature validation. Apple is aware of a report that this issue may have been actively exploited against versions of iOS before iOS 16.7.	5.5	More Details
CVE-2023-43616	An issue was discovered in Croc through 9.6.5. A sender can cause a receiver to overwrite files during ZIP extraction.	5.5	More Details
CVE-2023-36234	Cross Site Scripting (XSS) vulnerability in Netbox 3.5.1, allows attackers to execute arbitrary code via Name field in device-roles/add function.	5.4	More Details
CVE-2023-43456	Cross Site Scripting vulnerability in Service Provider Management System v.1.0 allows a remote attacker to execute arbitrary code and obtain sensitive information via the firstname, middlename and lastname parameters in the /php-spms/admin/?page=user endpoint.	5.4	More Details
CVE-2023-43495	Jenkins 2.423 and earlier, LTS 2.414.1 and earlier does not escape the value of the 'caption' constructor parameter of 'ExpandableDetailsNote', resulting in a stored cross-site scripting (XSS) vulnerability exploitable by attackers able to control this parameter.	5.4	More Details
CVE-2023-43499	Jenkins Build Failure Analyzer Plugin 2.4.1 and earlier does not escape Failure Cause names in build logs, resulting in a stored cross-site scripting (XSS) vulnerability exploitable by attackers able to create or update Failure Causes.	5.4	More Details

CVE Number	Description	Base Score	Reference
CVE-2023-43377	A cross-site scripting (XSS) vulnerability in /hoteldruid/visualizza_contratto.php of Hoteldruid v3.0.5 allows attackers to execute arbitrary web scripts or HTML via a crafted payload injected into the destinatario_email1 parameter.	5.4	More Details
CVE-2023-43458	Cross Site Scripting (XSS) vulnerability in Resort Reservation System v.1.0 allows a remote attacker to execute arbitrary code and obtain sensitive information via the room, name, and description parameters in the manage_room function.	5.4	More Details
CVE-2023-39575	A reflected cross-site scripting (XSS) vulnerability in the url_str URL parameter of ISL ARP Guard v4.0.2 allows attackers to execute arbitrary web scripts or HTML via a crafted payload.	5.4	More Details
CVE-2023-43376	A cross-site scripting (XSS) vulnerability in /hoteldruid/clienti.php of Hoteldruid v3.0.5 allows attackers to execute arbitrary web scripts or HTML via a crafted payload injected into the nometipotariffa1 parameter.	5.4	More Details
CVE-2023-42817	Pimcore admin-ui-classic-bundle provides a Backend UI for Pimcore. The translation value with text including “%s” (from “%suggest%) is parsed by sprintf() even though it’s supposed to be output literally to the user. The translations may be accessible by a user with comparatively lower overall access (as the translation permission cannot be scoped to certain “modules”) and a skilled attacker might be able to exploit the parsing of the translation string in the dialog box. This issue has been patched in commit `abd77392` which is included in release 1.1.2. Users are advised to update to version 1.1.2 or apply the patch manually.	5.4	More Details
CVE-2023-4631	The DoLogin Security WordPress plugin before 3.7 uses headers such as the X-Forwarded-For to retrieve the IP address of the request, which could lead to IP spoofing.	5.3	More Details
CVE-2023-4281	This Activity Log WordPress plugin before 2.8.8 retrieves client IP addresses from potentially untrusted headers, allowing an attacker to manipulate its value. This may be used to hide the source of malicious traffic.	5.3	More Details
CVE-2023-43617	An issue was discovered in Croc through 9.6.5. When a custom shared secret is used, the sender and receiver may divulge parts of this secret to an untrusted Relay, as part of composing a room name.	5.3	More Details
CVE-2023-43618	An issue was discovered in Croc through 9.6.5. The protocol requires a sender to provide its local IP addresses in cleartext via an ips? message.	5.3	More Details

CVE Number	Description	Base Score	Reference
CVE-2023-2508	The `PaperCutNG Mobility Print` version 1.0.3512 application allows an unauthenticated attacker to perform a CSRF attack on an instance administrator to configure the clients host (in the "configure printer discovery" section). This is possible because the application has no protections against CSRF attacks, like Anti-CSRF tokens, header origin validation, samesite cookies, etc.	5.3	More Details
CVE-2015-6964	MultiBit HD before 0.1.2 allows attackers to conduct bit-flipping attacks that insert unspendable Bitcoin addresses into the list that MultiBit uses to send fees to the developers. (Attackers cannot realistically steal these fees for themselves.) This occurs because there is no message authentication code (MAC).	5.3	More Details
CVE-2023-41295	Vulnerability of improper permission management in the displayengine module. Successful exploitation of this vulnerability may cause the screen to turn dim.	5.3	More Details
CVE-2023-4292	Frauscher Sensortechnik GmbH FDS101 for FAdC/FAdCi v1.4.24 and all previous versions are vulnerable to a SQL injection vulnerability via manipulated parameters of the web interface without authentication. The database contains limited, non-critical log information.	5.3	More Details
CVE-2023-26144	Versions of the package graphql from 16.3.0 and before 16.8.1 are vulnerable to Denial of Service (DoS) due to insufficient checks in the OverlappingFieldsCanBeMergedRule.ts file when parsing large queries. This vulnerability allows an attacker to degrade system performance. **Note:** It was not proven that this vulnerability can crash the process.	5.3	More Details
CVE-2023-31011	NVIDIA DGX H100 BMC contains a vulnerability in the REST service where an attacker may cause improper input validation. A successful exploit of this vulnerability may lead to escalation of privileges and information disclosure.	5.2	More Details
CVE-2023-41614	A stored cross-site scripting (XSS) vulnerability in the Add Animal Details function of Zoo Management System v1.0 allows attackers to execute arbitrary web scripts or HTML via a crafted payload injected into the Description of Animal parameter.	4.8	More Details
CVE-2023-41616	A reflected cross-site scripting (XSS) vulnerability in the Search Student function of Student Management System v1.2.3 and before allows attackers to execute arbitrary Javascript in the context of a victim user's browser via a crafted payload.	4.8	More Details
CVE-2023-43309	There is a stored cross-site scripting (XSS) vulnerability in Webmin 2.002 and below via the Cluster Cron Job tab Input field, which allows attackers to run malicious scripts by injecting a specially crafted payload.	4.8	More Details

CVE Number	Description	Base Score	Reference
CVE-2023-3226	The Popup Builder WordPress plugin before 4.2.0 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-2023-4502	The Translate WordPress with GTranslate WordPress plugin before 3.0.4 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). This vulnerability affects multiple parameters.	4.8	More Details
CVE-2023-42811	aes-gcm is a pure Rust implementation of the AES-GCM. Starting in version 0.10.0 and prior to version 0.10.3, in the AES GCM implementation of decrypt_in_place_detached, the decrypted ciphertext (i.e. the correct plaintext) is exposed even if tag verification fails. If a program using the `aes-gcm` crate's `decrypt_in_place*` APIs accesses the buffer after decryption failure, it will contain a decryption of an unauthenticated input. Depending on the specific nature of the program this may enable Chosen Ciphertext Attacks (CCAs) which can cause a catastrophic breakage of the cipher including full plaintext recovery. Version 0.10.3 contains a fix for this issue.	4.7	More Details
CVE-2023-43621	An issue was discovered in Croc through 9.6.5. The shared secret, located on a command line, can be read by local users who list all processes and their arguments.	4.7	More Details
CVE-2023-42482	Samsung Mobile Processor Exynos 2200 allows a GPU Use After Free.	4.7	More Details
CVE-2023-23766	An incorrect comparison vulnerability was identified in GitHub Enterprise Server that allowed commit smuggling by displaying an incorrect diff in a re-opened Pull Request. To do so, an attacker would need write access to the repository. This vulnerability affected all versions of GitHub Enterprise Server and was fixed in versions 3.6.17, 3.7.15, 3.8.8, 3.9.3, and 3.10.1. This vulnerability was reported via the GitHub Bug Bounty program.	4.5	More Details
CVE-2023-40368	IBM Storage Protect 8.1.0.0 through 8.1.19.0 could allow a privileged user to obtain sensitive information from the administrative command line client. IBM X-Force ID: 263456.	4.4	More Details
CVE-2023-20594	Improper initialization of variables in the DXE driver may allow a privileged user to leak sensitive information via local access.	4.4	More Details

CVE Number	Description	Base Score	Reference
CVE-2023-4156	A heap out-of-bounds read flaw was found in builtin.c in the gawk package. This issue may lead to a crash and could be used to read sensitive information.	4.4	More Details
CVE-2023-43494	Jenkins 2.50 through 2.423 (both inclusive), LTS 2.60.1 through 2.414.1 (both inclusive) does not exclude sensitive build variables (e.g., password parameter values) from the search in the build history widget, allowing attackers with Item/Read permission to obtain values of sensitive variables used in builds by iteratively testing different characters until the correct sequence is discovered.	4.3	More Details
CVE-2023-5134	The Easy Registration Forms for WordPress is vulnerable to Information Disclosure via the 'erforms_user_meta' shortcode in versions up to, and including, 2.1.1 due to insufficient controls on the information retrievable via the shortcode. This makes it possible for authenticated attackers, with subscriber-level capabilities or above, to retrieve arbitrary sensitive user meta.	4.3	More Details
CVE-2022-3962	A content spoofing vulnerability was found in Kiali. It was discovered that Kiali does not implement error handling when the page or endpoint being accessed cannot be found. This issue allows an attacker to perform arbitrary text injection when an error response is retrieved from the URL being accessed.	4.3	More Details
CVE-2022-4245	A flaw was found in codehaus-plexus. The org.codehaus.plexus.util.xml.XmlWriterUtil#writeComment fails to sanitize comments for a --> sequence. This issue means that text contained in the command string could be interpreted as XML and allow for XML injection.	4.3	More Details
CVE-2023-43502	A cross-site request forgery (CSRF) vulnerability in Jenkins Build Failure Analyzer Plugin 2.4.1 and earlier allows attackers to delete Failure Causes.	4.3	More Details
CVE-2023-31014	NVIDIA GeForce Now for Android contains a vulnerability in the game launcher component, where a malicious application on the same device can process the implicit intent meant for the streamer component. A successful exploit of this vulnerability may lead to limited information disclosure, denial of service, and code execution.	4.2	More Details
CVE-2023-4753	OpenHarmony v3.2.1 and prior version has a system call function usage error. Local attackers can crash kernel by the error input.	3.9	More Details
CVE-2023-5084	Cross-site Scripting (XSS) - Reflected in GitHub repository hestiacp/hestiacp prior to 1.8.8.	3.9	More Details

CVE Number	Description	Base Score	Reference
CVE-2023-38718	IBM Robotic Process Automation 21.0.0 through 21.0.7.8 could disclose sensitive information from access to RPA scripts, workflows and related data. IBM X-Force ID: 261606.	3.7	More Details
CVE-2023-5142	A vulnerability classified as problematic was found in H3C GR-1100-P, GR-1108-P, GR-1200W, GR-1800AX, GR-2200, GR-3200, GR-5200, GR-8300, ER2100n, ER2200G2, ER3200G2, ER3260G2, ER5100G2, ER5200G2 and ER6300G2 up to 20230908. This vulnerability affects unknown code of the file /userLogin.asp of the component Config File Handler. The manipulation leads to path traversal. The attack can be initiated remotely. The complexity of an attack is rather high. The exploitation appears to be difficult. The exploit has been disclosed to the public and may be used. VDB-240238 is the identifier assigned to this vulnerability. NOTE: The vendor was contacted early about this disclosure but did not respond in any way.	3.7	More Details
CVE-2023-41048	plone.namedfile allows users to handle `File` and `Image` fields targeting, but not depending on, Plone Dexterity content. Prior to versions 5.6.1, 6.0.3, 6.1.3, and 6.2.1, there is a stored cross site scripting vulnerability for SVG images. A security hotfix from 2021 already partially fixed this by making sure SVG images are always downloaded instead of shown inline. But the same problem still exists for scales of SVG images. Note that an image tag with an SVG image as source is not vulnerable, even when the SVG image contains malicious code. To exploit the vulnerability, an attacker would first need to upload an image, and then trick a user into following a specially crafted link. Patches are available in versions 5.6.1 (for Plone 5.2), 6.0.3 (for Plone 6.0.0-6.0.4), 6.1.3 (for Plone 6.0.5-6.0.6), and 6.2.1 (for Plone 6.0.7). There are no known workarounds.	3.7	More Details
CVE-2023-42458	Zope is an open-source web application server. Prior to versions 4.8.10 and 5.8.5, there is a stored cross site scripting vulnerability for SVG images. Note that an image tag with an SVG image as source is never vulnerable, even when the SVG image contains malicious code. To exploit the vulnerability, an attacker would first need to upload an image, and then trick a user into following a specially crafted link. Patches are available in Zope 4.8.10 and 5.8.5. As a workaround, make sure the "Add Documents, Images, and Files" permission is only assigned to trusted roles. By default, only the Manager has this permission.	3.7	More Details
CVE-2022-45448	M4 PDF plugin for Prestashop sites, in its 3.2.3 version and before, is vulnerable to an arbitrary HTML Document crafting vulnerability. The resource /m4pdf/pdf.php uses templates to dynamically create documents. In the case that the template does not exist, the application will return a fixed document with a message in mpdf format. An attacker could exploit this vulnerability by inputting a valid HTML/CSS document as the value of the parameter.	3.5	More Details

CVE Number	Description	Base Score	Reference
CVE-2023-34047	A batch loader function in Spring for GraphQL versions 1.1.0 - 1.1.5 and 1.2.0 - 1.2.2 may be exposed to GraphQL context with values, including security context values, from a different session. An application is vulnerable if it provides a DataLoaderOptions instance when registering batch loader functions through DefaultBatchLoaderRegistry.	3.1	More Details
CVE-2023-42456	Sudo-rs, a memory safe implementation of sudo and su, allows users to not have to enter authentication at every sudo attempt, but instead only requiring authentication every once in a while in every terminal or process group. Only once a configurable timeout has passed will the user have to re-authenticate themselves. Supporting this functionality is a set of session files (timestamps) for each user, stored in `/var/run/sudo-rs/ts`. These files are named according to the username from which the sudo attempt is made (the origin user). An issue was discovered in versions prior to 0.2.1 where usernames containing the `.` and `/` characters could result in the corruption of specific files on the filesystem. As usernames are generally not limited by the characters they can contain, a username appearing to be a relative path can be constructed. For example we could add a user to the system containing the username `../../../../bin/cp`. When logged in as a user with that name, that user could run `sudo -K` to clear their session record file. The session code then constructs the path to the session file by concatenating the username to the session file storage directory, resulting in a resolved path of `/bin/cp`. The code then clears that file, resulting in the `cp` binary effectively being removed from the system. An attacker needs to be able to login as a user with a constructed username. Given that such a username is unlikely to exist on an existing system, they will also need to be able to create the users with the constructed usernames. The issue is patched in version 0.2.1 of sudo-rs. Sudo-rs now uses the uid for the user instead of their username for determining the filename. Note that an upgrade to this version will result in existing session files being ignored and users will be forced to re-authenticate. It also fully eliminates any possibility of path traversal, given that uids are always integer values. The `sudo -K` and `sudo -k` commands can run, even if a user has no sudo access. As a workaround, make sure that one's system does not contain any users with a specially crafted username. While this is the case and while untrusted users do not have the ability to create arbitrary users on the system, one should not be able to exploit this issue.	3.1	More Details
CVE-2023-43764	Rejected reason: DO NOT USE THIS CANDIDATE NUMBER. ConsultIDs: CVE-2023-43762. Reason: This candidate is a duplicate of CVE-2023-43762. Notes: All CVE users should reference CVE-2023-43762 instead of this candidate. All references and descriptions in this candidate have been removed to prevent accidental usage.	N/A	More Details

CVE Number	Description	Base Score	Reference
CVE-2023-5129	Rejected reason: This CVE ID has been rejected or withdrawn by its CVE Numbering Authority. Duplicate of CVE-2023-4863.	N/A	More Details