SingCERT
Singapore Cyber Emergency Response Team

Security Bulletin 11 October 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-2023-4309	Election Services Co. (ESC) Internet Election Service is vulnerable to SQL injection in multiple pages and parameters. These vulnerabilities allow an unauthenticated, remote attacker to read or modify data for any elections that share the same backend database. ESC deactivated older and unused elections and enabled web application firewall (WAF) protection for current and future elections on or around 2023-08-12.	10.0	More Details
CVE-2023-2306	Qognify NiceVision versions 3.1 and prior are vulnerable to exposing sensitive information using hard-coded credentials. With these credentials an attacker can retrieve information about the cameras, user information, and modify database records.	10.0	More Details

CVE Number	Description	Base Score	Reference
CVE-2023-41094	TouchLink packets processed after timeout or out of range due to Operation on a Resource after Expiration and Missing Release of Resource after Effective Lifetime may allow a device to be added outside of valid TouchLink range or pairing duration This issue affects Ember ZNet 7.1.x from 7.1.3 through 7.1.5; 7.2.x from 7.2.0 through 7.2.3; Version 7.3 and later are unaffected	10.0	More Details
CVE-2022-36276	TCMAN GIM v8.0.1 is vulnerable to a SQL injection via the 'SqlWhere' parameter inside the function 'BuscarESM'. The exploitation of this vulnerability might allow a remote attacker to directly interact with the database.	9.9	More Details
CVE-2023-41373	A directory traversal vulnerability exists in the BIG-IP Configuration Utility that may allow an authenticated attacker to execute commands on the BIG-IP system. For BIG-IP system running in Appliance mode, a successful exploit can allow the attacker to cross a security boundary. Note: Software versions which have reached End of Technical Support (EoTS) are not evaluated.	9.9	More Details
CVE-2023-3701	Aqua Drive, in its 2.4 version, is vulnerable to a relative path traversal vulnerability. By exploiting this vulnerability, an authenticated non privileged user could access/modify stored resources of other users. It could also be possible to access and modify the source and configuration files of the cloud disk platform, affecting the integrity and availability of the entire platform.	9.9	More Details
CVE-2023-4037	Blind SQL injection vulnerability in the Conacwin 3.7.1.2 web interface, the exploitation of which could allow a local attacker to obtain sensitive data stored in the database by sending a specially crafted SQL query to the xml parameter.	9.9	More Details
CVE-2023-3038	SQL injection vulnerability in HelpDezk Community affecting version 1.1.10. This vulnerability could allow a remote attacker to send a specially crafted SQL query to the rows parameter of the jsonGrid route and extract all the information stored in the application.	9.8	More Details
CVE-2023-4494	Stack-based buffer overflow vulnerability in Easy Chat Server 3.1 version. An attacker could send an excessively long username string to the register.ghp file asking for the name via a GET request resulting in arbitrary code execution on the remote machine.	9.8	More Details
CVE-2023-44467	langchain_experimental (aka LangChain Experimental) in LangChain before 0.0.306 allows an attacker to bypass the CVE-2023-36258 fix and execute arbitrary code via __import__ in Python code, which is not prohibited by pal_chain/base.py.	9.8	More Details

CVE Number	Description	Base Score	Reference
CVE-2023-43899	hansun CMS v1.0 was discovered to contain a SQL injection vulnerability via the component /ajax/ajax_login.ashx.	9.8	More Details
CVE-2023-36380	A vulnerability has been identified in CP-8031 MASTER MODULE (All versions < CPCI85 V05.11 (only with activated debug support)), CP-8050 MASTER MODULE (All versions < CPCI85 V05.11 (only with activated debug support)). The affected devices contain a hard-coded ID in the SSH `authorized_keys` configuration file. An attacker with knowledge of the corresponding private key could login to the device via SSH. Only devices with activated debug support are affected.	9.8	More Details
CVE-2023-43625	A vulnerability has been identified in Simcenter Amesim (All versions < V2021.1). The affected application contains a SOAP endpoint that could allow an unauthenticated remote attacker to perform DLL injection and execute arbitrary code in the context of the affected application process.	9.8	More Details
CVE-2023-30801	All versions of the qBittorrent client through 4.5.5 use default credentials when the web user interface is enabled. The administrator is not forced to change the default credentials. As of 4.5.5, this issue has not been fixed. A remote attacker can use the default credentials to authenticate and execute arbitrary operating system commands using the "external program" feature in the web user interface. This was reportedly exploited in the wild in March 2023.	9.8	More Details
CVE-2023-30803	The Sangfor Next-Gen Application Firewall version NGAF8.0.17 is vulnerable to an authentication bypass vulnerability. A remote and unauthenticated attacker can bypass authentication and access administrative functionality by sending HTTP requests using a crafted Y-forwarded-for header.	9.8	More Details
CVE-2023-30805	The Sangfor Next-Gen Application Firewall version NGAF8.0.17 is vulnerable to an operating system command injection vulnerability. A remote and unauthenticated attacker can execute arbitrary commands by sending a crafted HTTP POST request to the /LogInOut.php endpoint. This is due to mishandling of shell meta-characters in the "un" parameter.	9.8	More Details
CVE-2023-30806	The Sangfor Next-Gen Application Firewall version NGAF8.0.17 is vulnerable to an operating system command injection vulnerability. A remote and unauthenticated attacker can execute arbitrary commands by sending a crafted HTTP POST request to the /cgi-bin/login.cgi endpoint. This is due to mishandling of shell meta-characters in the PHPSESSID cookie.	9.8	More Details

CVE Number	Description	Base Score	Reference
CVE-2023-22515	Atlassian has been made aware of an issue reported by a handful of customers where external attackers may have exploited a previously unknown vulnerability in publicly accessible Confluence Data Center and Server instances to create unauthorized Confluence administrator accounts and access Confluence instances. Atlassian Cloud sites are not affected by this vulnerability. If your Confluence site is accessed via an atlassian.net domain, it is hosted by Atlassian and is not vulnerable to this issue.	9.8	More Details
CVE-2020-27630	In Silicon Labs uC/TCP-IP 3.6.0, TCP ISNs are improperly random.	9.8	More Details
CVE-2020-27631	In Oryx CycloneTCP 1.9.6, TCP ISNs are improperly random.	9.8	More Details
CVE-2023-34992	A improper neutralization of special elements used in an os command ('os command injection') in Fortinet FortiSIEM version 7.0.0 and 6.7.0 through 6.7.5 and 6.6.0 through 6.6.3 and 6.5.0 through 6.5.1 and 6.4.0 through 6.4.2 allows attacker to execute unauthorized code or commands via crafted API requests.	9.8	More Details
CVE-2023-34993	A improper neutralization of special elements used in an os command ('os command injection') in Fortinet FortiWLM version 8.6.0 through 8.6.5 and 8.5.0 through 8.5.4 allows attacker to execute unauthorized code or commands via specifically crafted http get request parameters.	9.8	More Details
CVE-2023-36547	A improper neutralization of special elements used in an os command ('os command injection') in Fortinet FortiWLM version 8.6.0 through 8.6.5 and 8.5.0 through 8.5.4 allows attacker to execute unauthorized code or commands via specifically crafted http get request parameters.	9.8	More Details
CVE-2023-36548	A improper neutralization of special elements used in an os command ('os command injection') in Fortinet FortiWLM version 8.6.0 through 8.6.5 and 8.5.0 through 8.5.4 allows attacker to execute unauthorized code or commands via specifically crafted http get request parameters.	9.8	More Details
CVE-2023-36550	A improper neutralization of special elements used in an os command ('os command injection') in Fortinet FortiWLM version 8.6.0 through 8.6.5 and 8.5.0 through 8.5.4 allows attacker to execute unauthorized code or commands via specifically crafted http get request parameters.	9.8	More Details
CVE-2023-35349	Microsoft Message Queuing (MSMQ) Remote Code Execution Vulnerability	9.8	More Details

CVE Number	Description	Base Score	Reference
CVE-2023-36434	Windows IIS Server Elevation of Privilege Vulnerability	9.8	More Details
CVE-2023-45199	Mbed TLS 3.2.x through 3.4.x before 3.5 has a Buffer Overflow that can lead to remote Code execution.	9.8	More Details
CVE-2023-5365	HP LIFE Android Mobile application is potentially vulnerable to escalation of privilege and/or information disclosure.	9.8	More Details
CVE-2023-45239	A lack of input validation exists in tac_plus prior to commit 4fdf178 which, when pre or post auth commands are enabled, allows an attacker who can control the username, rem-addr, or NAC address sent to tac_plus to inject shell commands and gain remote code execution on the tac_plus server.	9.8	More Details
CVE-2023-43981	Presto Changeo testsitecreator up to 1.1.1 was discovered to contain a deserialization vulnerability via the component delete_excluded_folder.php.	9.8	More Details
CVE-2023-20101	A vulnerability in Cisco Emergency Responder could allow an unauthenticated, remote attacker to log in to an affected device using the root account, which has default, static credentials that cannot be changed or deleted. This vulnerability is due to the presence of static user credentials for the root account that are typically reserved for use during development. An attacker could exploit this vulnerability by using the account to log in to an affected system. A successful exploit could allow the attacker to log in to the affected system and execute arbitrary commands as the root user.	9.8	More Details
CVE-2023-5402	A CWE-269: Improper Privilege Management vulnerability exists that could cause a remote code execution when the transfer command is used over the network.	9.8	More Details
CVE-2023-5391	A CWE-502: Deserialization of untrusted data vulnerability exists that could allow an attacker to execute arbitrary code on the targeted system by sending a specifically crafted packet to the application.	9.8	More Details
CVE-2023-5399	A CWE-22: Improper Limitation of a Pathname to a Restricted Directory ('Path Traversal') vulnerability exists that could cause tampering of files on the personal computer running C-Bus when using the File Command.	9.8	More Details

CVE Number	Description	Base Score	Reference
CVE-2023-36619	Atos Unify OpenScape Session Border Controller through V10 R3.01.03 allows execution of administrative scripts by unauthenticated users.	9.8	More Details
CVE-2023-4491	Buffer overflow vulnerability in Easy Address Book Web Server 1.6 version. The exploitation of this vulnerability could allow an attacker to send a very long username string to /searchbook.ghp, asking for the name via a POST request, resulting in arbitrary code execution on the remote machine.	9.8	More Details
CVE-2023-35803	IQ Engine before 10.6r2 on Extreme Network AP devices has a Buffer Overflow.	9.8	More Details
CVE-2023-44807	D-Link DIR-820L 1.05B03 has a stack overflow vulnerability in the cancelPing function.	9.8	More Details
CVE-2023-40920	Prixan prixanconnect up to v1.62 was discovered to contain a SQL injection vulnerability via the component CartsGuruCatalogModuleFrontController::importProducts().	9.8	More Details
CVE-2023-32485	Dell SmartFabric Storage Software version 1.3 and lower contain an improper input validation vulnerability. A remote unauthenticated attacker may exploit this vulnerability and escalate privileges up to the highest administration level. This is a critical severity vulnerability affecting user authentication. Dell recommends customers to upgrade at the earliest opportunity.	9.8	More Details
CVE-2023-45311	fsevents before 1.2.11 depends on the https://fsevents-binaries.s3-us-west-2.amazonaws.com URL, which might allow an adversary to execute arbitrary code if any JavaScript project (that depends on fsevents) distributes code that was obtained from that URL at a time when it was controlled by an adversary. NOTE: some sources feel that this means that no version is affected any longer, because the URL is not controlled by an adversary.	9.8	More Details
CVE-2023-43983	Presto Changeo attributegrid up to 2.0.3 was discovered to contain a SQL injection vulnerability via the component disable_json.php.	9.8	More Details

CVE Number	Description	Base Score	Reference
CVE-2023-38703	PJSIP is a free and open source multimedia communication library written in C with high level API in C, C++, Java, C#, and Python languages. SRTP is a higher level media transport which is stacked upon a lower level media transport such as UDP and ICE. Currently a higher level transport is not synchronized with its lower level transport that may introduce use-after-free issue. This vulnerability affects applications that have SRTP capability (`PJMEDIA_HAS_SRTP` is set) and use underlying media transport other than UDP. This vulnerability's impact may range from unexpected application termination to control flow hijack/memory corruption. The patch is available as a commit in the master branch.	9.8	More Details
CVE-2023-44024	SQL injection vulnerability in KnowBand Module One Page Checkout, Social Login & Mailchimp (supercheckout) v.8.0.3 and before allows a remote attacker to execute arbitrary code via a crafted request to the updateCheckoutBehaviour function in the supercheckout.php component.	9.8	More Details
CVE-2023-43269	pigcms up to 7.0 was discovered to contain an arbitrary file upload vulnerability.	9.8	More Details
CVE-2023-4530	Improper Neutralization of Special Elements used in an SQL Command ('SQL Injection') vulnerability in Turna Advertising Administration Panel allows SQL Injection.This issue affects Advertising Administration Panel: before 1.1.	9.8	More Details
CVE-2023-42809	Redisson is a Java Redis client that uses the Netty framework. Prior to version 3.22.0, some of the messages received from the Redis server contain Java objects that the client deserializes without further validation. Attackers that manage to trick clients into communicating with a malicious server can include especially crafted objects in its responses that, once deserialized by the client, force it to execute arbitrary code. This can be abused to take control of the machine the client is running in. Version 3.22.0 contains a patch for this issue. Some post-fix advice is available. Do NOT use `Kryo5Codec` as deserialization codec, as it is still vulnerable to arbitrary object deserialization due to the `setRegistrationRequired(false)` call. On the contrary, `KryoCodec` is safe to use. The fix applied to `SerializationCodec` only consists of adding an optional allowlist of class names, even though making this behavior the default is recommended. When instantiating `SerializationCodec` please use the `SerializationCodec(ClassLoader classLoader, Set<String> allowedClasses)` constructor to restrict the allowed classes for deserialization.	9.6	More Details
CVE-2023-4966	Sensitive information disclosure in NetScaler ADC and NetScaler Gateway when configured as a Gateway (VPN virtual server, ICA Proxy, CVPN, RDP Proxy) or AAA virtual server.	9.4	More Details

CVE Number	Description	Base Score	Reference
CVE-2023-44393	Piwigo is an open source photo gallery application. Prior to version 14.0.0beta4, a reflected cross-site scripting (XSS) vulnerability is in the` /admin.php?page=plugins&tab=new&installstatus=ok&plugin_id=[here]` page. This vulnerability can be exploited by an attacker to inject malicious HTML and JS code into the HTML page, which could then be executed by admin users when they visit the URL with the payload. The vulnerability is caused by the insecure injection of the `plugin_id` value from the URL into the HTML page. An attacker can exploit this vulnerability by crafting a malicious URL that contains a specially crafted `plugin_id` value. When a victim who is logged in as an administrator visits this URL, the malicious code will be injected into the HTML page and executed. This vulnerability can be exploited by any attacker who has access to a malicious URL. However, only users who are logged in as administrators are affected. This is because the vulnerability is only present on the `/admin.php?page=plugins&tab=new&installstatus=ok&plugin_id=[here]` page, which is only accessible to administrators. Version 14.0.0.beta4 contains a patch for this issue.	9.3	More Details
CVE-2020-27635	In PicoTCP 1.7.0, TCP ISNs are improperly random.	9.1	More Details
CVE-2020-27634	In Contiki 4.5, TCP ISNs are improperly random.	9.1	More Details
CVE-2020-27633	In FNET 4.6.3, TCP ISNs are improperly random.	9.1	More Details
CVE-2023-43271	Incorrect access control in 70mai a500s v1.2.119 allows attackers to directly access and delete the video files of the driving recorder through ftp and other protocols.	9.1	More Details
CVE-2023-36465	Decidim is a participatory democracy framework, written in Ruby on Rails, originally developed for the Barcelona City government online and offline participation website. The `templates` module doesn't enforce the correct permissions, allowing any logged-in user to access to this functionality in the administration panel. An attacker could use this vulnerability to change, create or delete templates of surveys. This issue has been patched in version 0.26.8 and 0.27.4.	9.1	More Details

CVE Number	Description	Base Score	Reference
CVE-2023-38701	Hydra is the layer-two scalability solution for Cardano. Users of the Hydra head protocol send the UTxOs they wish to commit into the Hydra head first to the `commit` validator, where they remain until they are either collected into the `head` validator or the protocol initialisation is aborted and the value in the committed UTxOs is returned to the users who committed them. Prior to version 0.12.0, the `commit` validator contains a flawed check when the `ViaAbort` redeemer is used, which allows any user to spend any UTxO which is at the validator arbitrarily, meaning an attacker can steal the funds that users are trying to commit into the head validator. The intended behavior is that the funds must be returned to the user which committed the funds and can only be performed by a participant of the head. The `initial` validator also is similarly affected as the same flawed check is performed for the `ViaAbort` redeemer. Due to this issue, an attacker can steal any funds that user's try to commit into a Hydra head. Also, an attacker can prevent any Hydra head from being successfully opened. It does not allow an attacker to take funds which have been successfully collected into and currently reside in the `head` validator. Version 0.12.0 contains a fix for this issue.	9.1	More Details
CVE-2023-44208	Sensitive information disclosure and manipulation due to missing authorization. The following products are affected: Acronis Cyber Protect Home Office (Windows) before build 40713.	9.1	More Details
CVE-2020-27636	In Microchip MPLAB Net 3.6.1, TCP ISNs are improperly random.	9.1	More Details

OTHER VULNERABILITIES

CVE Number	Description	Base Score	Reference
CVE-2023-36556	An incorrect authorization vulnerability [CWE-863] in FortiMail webmail version 7.2.0 through 7.2.2, version 7.0.0 through 7.0.5 and below 6.4.7 allows an authenticated attacker to login on other users accounts from the same web domain via crafted HTTP or HTTPs requests.	8.8	More Details
CVE-2023-45208	A command injection in the parsing_xml_stasurvey function inside libcgifunc.so of the D-Link DAP-X1860 repeater 1.00 through 1.01b05-01 allows attackers (within range of the repeater) to run shell commands as root during the setup process of the repeater, via a crafted SSID. Also, network names containing single quotes (in the range of the repeater) can result in a denial of service.	8.8	More Details

CVE Number	Description	Base Score	Reference
CVE-2023-45160	In the affected version of the 1E Client, an ordinary user could subvert downloaded instruction resource files, e.g., to substitute a harmful script. by replacing a resource script file created by an instruction at run time with a malicious script. The 1E Client's temporary directory is now locked down in the released patch. Resolution: This has been fixed in patch Q23094 This issue has also been fixed in the Mac Client in updated versions of Non-Windows release v8.1.2.62 - please re-download from the 1E Support site. Customers with Mac Client versions higher than v8.1 will need to upgrade to v23.11 to remediate this vulnerability.	8.8	More Details
CVE-2023-44846	An issue in SeaCMS v.12.8 allows an attacker to execute arbitrary code via the admin_ notify.php component.	8.8	More Details
CVE-2023-45354	Atos Unify OpenScape Common Management Portal V10 before V10 R4.17.0 and V10 R5.1.0 allows an authenticated remote attacker to execute arbitrary code on the operating system by using the Common Management Portal web interface. This is also known as OCMP-6589.	8.8	More Details
CVE-2023-44827	An issue in ZenTao Community Edition v.18.6 and before, ZenTao Biz v.8.6 and before, ZenTao Max v.4.7 and before allows an attacker to execute arbitrary code via a crafted script to the Office Conversion Settings function.	8.8	More Details
CVE-2023-43284	D-Link Wireless MU-MIMO Gigabit AC1200 Router DIR-846 100A53DBR-Retail devices allow an authenticated remote attacker to execute arbitrary code via an unspecified manipulation of the QoS POST parameter.	8.8	More Details
CVE-2023-4997	Improper authorisation of regular users in ProIntegra Uptime DC software (versions below 2.0.0.33940) allows them to change passwords of all other users including administrators leading to a privilege escalation.	8.8	More Details
CVE-2023-44959	An issue found in D-Link DSL-3782 v.1.03 and before allows remote authenticated users to execute arbitrary code as root via the Router IP Address fields of the network settings page.	8.8	More Details
CVE-2023-44811	Cross Site Request Forgery (CSRF) vulnerability in MooSocial v.3.1.8 allows a remote attacker to execute arbitrary code and obtain sensitive information via the admin Password Change Function.	8.8	More Details

CVE Number	Description	Base Score	Reference
CVE-2023-43641	libcue provides an API for parsing and extracting data from CUE sheets. Versions 2.2.1 and prior are vulnerable to out-of-bounds array access. A user of the GNOME desktop environment can be exploited by downloading a cue sheet from a malicious webpage. Because the file is saved to `~/Downloads`, it is then automatically scanned by tracker-miners. And because it has a .cue filename extension, tracker-miners use libcue to parse the file. The file exploits the vulnerability in libcue to gain code execution. This issue is patched in version 2.3.0.	8.8	More Details
CVE-2023-4570	An improper access restriction in NI MeasurementLink Python services could allow an attacker on an adjacent network to reach services exposed on localhost. These services were previously thought to be unreachable outside of the node. This affects measurement plug-ins written in Python using version 1.1.0 of the ni-measurementlink-service Python package and all previous versions.	8.8	More Details
CVE-2023-39928	A use-after-free vulnerability exists in the MediaRecorder API of Webkit WebKitGTK 2.40.5. A specially crafted web page can abuse this vulnerability to cause memory corruption and potentially arbitrary code execution. A user would need to to visit a malicious webpage to trigger this vulnerability.	8.8	More Details
CVE-2023-5346	Type confusion in V8 in Google Chrome prior to 117.0.5938.149 allowed a remote attacker to potentially exploit heap corruption via a crafted HTML page. (Chromium security severity: High)	8.8	More Details
CVE-2023-34988	A improper neutralization of special elements used in an os command ('os command injection') in Fortinet FortiWLM version 8.6.0 through 8.6.5 and 8.5.0 through 8.5.4 allows attacker to execute unauthorized code or commands via specifically crafted HTTP get request parameters.	8.8	More Details
CVE-2023-45350	Atos Unify OpenScape 4000 Manager V10 R1 before V10 R1.42.1 and 4000 Manager V10 R0 allow Privilege escalation that may lead to the ability of an authenticated attacker to run arbitrary code via AScm. This is also known as OSFOURK-24034.	8.8	More Details
CVE-2023-34987	A improper neutralization of special elements used in an os command ('os command injection') in Fortinet FortiWLM version 8.6.0 through 8.6.5 and 8.5.0 through 8.5.4 allows attacker to execute unauthorized code or commands via specifically crafted HTTP get request parameters.	8.8	More Details
CVE-2023-34986	A improper neutralization of special elements used in an os command ('os command injection') in Fortinet FortiWLM version 8.6.0 through 8.6.5 and 8.5.0 through 8.5.4 allows attacker to execute unauthorized code or commands via specifically crafted HTTP get request parameters.	8.8	More Details

CVE Number	Description	Base Score	Reference
CVE-2023-34985	A improper neutralization of special elements used in an os command ('os command injection') in Fortinet FortiWLM version 8.6.0 through 8.6.5 and 8.5.0 through 8.5.4 allows attacker to execute unauthorized code or commands via specifically crafted HTTP get request parameters.	8.8	More Details
CVE-2023-44061	File Upload vulnerability in Simple and Nice Shopping Cart Script v.1.0 allows a remote attacker to execute arbitrary code via the upload function in the edit profile component.	8.8	More Details
CVE-2023-45352	Atos Unify OpenScape Common Management Portal V10 before V10 R4.17.0 and V10 R5.1.0 allows an authenticated attacker to execute arbitrary code on the operating system via a Common Management Portal web interface Path traversal vulnerability allowing write access outside the intended folders. This is also known as OCMP-6592.	8.8	More Details
CVE-2023-4837	SmodBIP is vulnerable to Cross-Site Request Forgery, that could be used to induce logged in users to perform unintended actions, including creation of additional accounts with administrative privileges. This issue affects all versions of SmodBIP. SmodBIP is no longer maintained and the vulnerability will not be fixed.	8.8	More Details
CVE-2023-34989	A improper neutralization of special elements used in an os command ('os command injection') in Fortinet FortiWLM version 8.6.0 through 8.6.5 and 8.5.0 through 8.5.4 allows attacker to execute unauthorized code or commands via specifically crafted HTTP get request parameters.	8.8	More Details
CVE-2023-45351	Atos Unify OpenScape 4000 Assistant V10 R1 before V10 R1.42.1, 4000 Assistant V10 R0, 4000 Manager V10 R1 before V10 R1.42.1, and 4000 Manager V10 R0 allow Authenticated Command Injection via AShbr. This is also known as OSFOURK-24039.	8.8	More Details
CVE-2023-45356	Atos Unify OpenScape 4000 Platform V10 R1 before Hotfix V10 R1.42.2 4000 and Manager Platform V10 R1 before Hotfix V10 R1.42.2 allow command injection by an authenticated attacker into the platform operating system, leading to administrative access, via dtb pages of the platform portal. This is also known as OSFOURK-23719.	8.8	More Details
CVE-2023-45312	In the mtproto_proxy (aka MTProto proxy) component through 0.7.2 for Erlang, a low-privileged remote attacker can access an improperly secured default installation without authenticating and achieve remote command execution ability.	8.8	More Details
CVE-2023-36414	Azure Identity SDK Remote Code Execution Vulnerability	8.8	More Details

CVE Number	Description	Base Score	Reference
CVE-2023-45353	Atos Unify OpenScape Common Management Portal V10 before V10 R4.17.0 and V10 R5.1.0 allows an authenticated attacker to execute arbitrary code on the operating system by leveraging the Common Management Portal web interface for Authenticated remote upload and creation of arbitrary files affecting the underlying operating system. This is also known as OCMP-6591.	8.8	More Details
CVE-2023-36415	Azure Identity SDK Remote Code Execution Vulnerability	8.8	More Details
CVE-2023-36577	Microsoft WDAC OLE DB provider for SQL Server Remote Code Execution Vulnerability	8.8	More Details
CVE-2023-45355	Atos Unify OpenScape 4000 Platform V10 R1 before Hotfix V10 R1.42.2 and 4000 and Manager Platform V10 R1 before Hotfix V10 R1.42.2 allow command injection by an authenticated attacker into the platform operating system, leading to administrative access via the webservice. This is also known as OSFOURK-24120.	8.8	More Details
CVE-2023-36419	Azure HDInsight Apache Oozie Workflow Scheduler XXE Elevation of Privilege Vulnerability	8.8	More Details
CVE-2023-36618	Atos Unify OpenScape Session Border Controller through V10 R3.01.03 allows execution of OS commands as root user by low-privileged authenticated users.	8.8	More Details
CVE-2023-36549	A improper neutralization of special elements used in an os command ('os command injection') in Fortinet FortiWLM version 8.6.0 through 8.6.5 and 8.5.0 through 8.5.4 allows attacker to execute unauthorized code or commands via specifically crafted http get request parameters.	8.8	More Details
CVE-2023-42455	Wazuh is a security detection, visibility, and compliance open source project. In versions 4.4.0 and 4.4.1, it is possible to get the Wazuh API administrator key used by the Dashboard using the browser development tools. This allows a logged user to the dashboard to become administrator of the API, even if their dashboard role is not. Version 4.4.2 contains a fix. There are no known workarounds.	8.8	More Details
CVE-2023-43321	File Upload vulnerability in Digital China Networks DCFW-1800-SDC v.3.0 allows an authenticated attacker to execute arbitrary code via the wget function in the /sbin/cloudadmin.sh component.	8.8	More Details

CVE Number	Description	Base Score	Reference
CVE-2023-43746	When running in Appliance mode, an authenticated user assigned the Administrator role may be able to bypass Appliance mode restrictions, utilizing BIG-IP external monitor on a BIG-IP system. A successful exploit can allow the attacker to cross a security boundary. Note: Software versions which have reached End of Technical Support (EoTS) are not evaluated.	8.7	More Details
CVE-2023-20259	A vulnerability in an API endpoint of multiple Cisco Unified Communications Products could allow an unauthenticated, remote attacker to cause high CPU utilization, which could impact access to the web-based management interface and cause delays with call processing. This API is not used for device management and is unlikely to be used in normal operations of the device. This vulnerability is due to improper API authentication and incomplete validation of the API request. An attacker could exploit this vulnerability by sending a crafted HTTP request to a specific API on the device. A successful exploit could allow the attacker to cause a denial of service (DoS) condition due to high CPU utilization, which could negatively impact user traffic and management access. When the attack stops, the device will recover without manual intervention.	8.6	More Details
CVE-2023-3037	Improper authorization vulnerability in HelpDezk Community affecting version 1.1.10. This vulnerability could allow a remote attacker to access the platform without authentication and retrieve personal data via the jsonGrid parameter.	8.6	More Details
CVE-2023-45612	In JetBrains Ktor before 2.3.5 default configuration of ContentNegotiation with XML format was vulnerable to XXE	8.6	More Details
CVE-2023-30692	Improper input validation vulnerability in Evaluator prior to SMR Oct-2023 Release 1 allows local attackers to launch privileged activities.	8.5	More Details
CVE-2023-41679	An improper access control vulnerability [CWE-284] in FortiManager management interface 7.2.0 through 7.2.2, 7.0.0 through 7.0.7, 6.4.0 through 6.4.11, 6.2 all versions, 6.0 all versions may allow a remote and authenticated attacker with at least "device management" permission on his profile and belonging to a specific ADOM to add and delete CLI script on other ADOMs	8.5	More Details
CVE-2023-30690	Improper input validation vulnerability in Duo prior to SMR Oct-2023 Release 1 allows local attackers to launch privileged activities.	8.5	More Details

CVE Number	Description	Base Score	Reference
CVE-2023-45159	1E Client installer can perform arbitrary file deletion on protected files. A non-privileged user could provide a symbolic link or Windows junction to point to a protected directory in the installer that the 1E Client would then clear on service startup. A hotfix is available from the 1E support portal that forces the 1E Client to check for a symbolic link or junction and if it finds one refuses to use that path and instead creates a path involving a random GUID. for v8.1 use hotfix Q23097 for v8.4 use hotfix Q23105 for v9.0 use hotfix Q23115 for SaaS customers, use 1EClient v23.7 plus hotfix Q23121	8.4	More Details
CVE-2023-35897	IBM Spectrum Protect Client and IBM Storage Protect for Virtual Environments 8.1.0.0 through 8.1.19.0 could allow a local user to execute arbitrary code on the system using a specially crafted file, caused by a DLL hijacking flaw. IBM X-Force ID: 259246.	8.4	More Details
CVE-2023-45303	ThingsBoard before 3.5 allows Server-Side Template Injection if users are allowed to modify an email template, because Apache FreeMarker supports freemarker.template.utility.Execute (for content sent to the /api/admin/settings endpoint).	8.4	More Details
CVE-2023-36569	Microsoft Office Elevation of Privilege Vulnerability	8.4	More Details
CVE-2023-35796	A vulnerability has been identified in SINEMA Server V14 (All versions). The affected application improperly sanitizes certain SNMP configuration data retrieved from monitored devices. An attacker with access to a monitored device could perform a stored cross-site scripting (XSS) attack that may lead to arbitrary code execution with `SYSTEM` privileges on the application server. (ZDI-CAN-19823)	8.3	More Details
CVE-2023-26153	Versions of the package geokit-rails before 2.5.0 are vulnerable to Command Injection due to unsafe deserialisation of YAML within the 'geo_location' cookie. This issue can be exploited remotely via a malicious cookie value. **Note:** An attacker can use this vulnerability to execute commands on the host system.	8.3	More Details
CVE-2023-43696	Improper Access Control in SICK APU allows an unprivileged remote attacker to download as well as upload arbitrary files via anonymous access to the FTP server.	8.2	More Details

CVE Number	Description	Base Score	Reference
CVE-2023-39191	An improper input validation flaw was found in the eBPF subsystem in the Linux kernel. The issue occurs due to a lack of proper validation of dynamic pointers within user-supplied eBPF programs prior to executing them. This may allow an attacker with CAP_BPF privileges to escalate privileges and execute arbitrary code in the context of the kernel.	8.2	More Details
CVE-2023-44392	Garden provides automation for Kubernetes development and testing. Prior tov ersions 0.13.17 and 0.12.65, Garden has a dependency on the cryo library, which is vulnerable to code injection due to an insecure implementation of deserialization. Garden stores serialized objects using cryo in the Kubernetes `ConfigMap` resources prefixed with `test-result` and `run-result` to cache Garden test and run results. These `ConfigMaps` are stored either in the `garden-system` namespace or the configured user namespace. When a user invokes the command `garden test` or `garden run` objects stored in the `ConfigMap` are retrieved and deserialized. This can be used by an attacker with access to the Kubernetes cluster to store malicious objects in the `ConfigMap`, which can trigger a remote code execution on the users machine when cryo deserializes the object. In order to exploit this vulnerability, an attacker must have access to the Kubernetes cluster used to deploy garden remote environments. Further, a user must actively invoke either a `garden test` or `garden run` which has previously cached results. The issue has been patched in Garden versions `0.13.17` (Bonsai) and `0.12.65` (Acorn). Only Garden versions prior to these are vulnerable. No known workarounds are available.	8.2	More Details
CVE-2023-44848	An issue in SeaCMS v.12.8 allows an attacker to execute arbitrary code via the admin_template.php component.	8.1	More Details
CVE-2023-42448	Hydra is the layer-two scalability solution for Cardano. Prior to version 0.13.0, the specification states that the contestation period in the datum of the UTxO at the head validator must stay unchanged as the state progresses from Open to Closed (Close transaction), but no such check appears to be performed in the `checkClose` function of the head validator. This would allow a malicious participant to modify the contestation deadline of the head to either allow them to fanout the head without giving another participant the chance to contest, or prevent any participant from ever redistributing the funds locked in the head via a fan-out. Version 0.13.0 contains a patch for this issue.	8.1	More Details

CVE Number	Description	Base Score	Reference
CVE-2023-42449	Hydra is the two-layer scalability solution for Cardano. Prior to version 0.13.0, it is possible for a malicious head initializer to extract one or more PTs for the head they are initializing due to incorrect data validation logic in the head token minting policy which then results in an flawed check for burning the head ST in the `initial` validator. This is possible because it is not checked in `HeadTokens.hs` that the datums of the outputs at the `initial` validator are equal to the real head ID, and it is also not checked in the `off-chain code`. During the `Initial` state of the protocol, if the malicious initializer removes a PT from the Hydra scripts it becomes impossible for any other participant to reclaim any funds they have attempted to commit into the head, as to do so the Abort transaction must burn all the PTs for the head, but they cannot burn the PT which the attacker controls and so cannot satisfy this requirement. That means the initializer can lock the other participants committed funds forever or until they choose to return the PT (ransom). The malicious initializer can also use the PT to spoof that they have committed a particular TxO when progressing the head into the `Open` state. For example, they could say they committed a TxO residing at their address containing 100 ADA, but in fact this 100 ADA was not moved into the head, and thus in order for an other participant to perform the fanout they will be forced to pay the attacker the 100 ADA out of their own funds, as the fanout transaction must pay all the committed TxOs (even though the attacker did not really commit that TxO). They can do this by placing the PT in a UTxO with a well-formed `Commit` datum with whatever contents they like, then use this UTxO in the `collectCom` transaction. There may be other possible ways to abuse having control of a PT. Version 0.13.0 fixes this issue.	8.1	More Details
CVE-2023-41841	An improper authorization vulnerability in Fortinet FortiOS 7.0.0 - 7.0.11 and 7.2.0 - 7.2.4 allows an attacker belonging to the prof-admin profile to perform elevated actions.	8.1	More Details
CVE-2023-41769	Layer 2 Tunneling Protocol Remote Code Execution Vulnerability	8.1	More Details
CVE-2023-41774	Layer 2 Tunneling Protocol Remote Code Execution Vulnerability	8.1	More Details
CVE-2023-38166	Layer 2 Tunneling Protocol Remote Code Execution Vulnerability	8.1	More Details
CVE-2023-41773	Layer 2 Tunneling Protocol Remote Code Execution Vulnerability	8.1	More Details

CVE Number	Description	Base Score	Reference
CVE-2023-39323	Line directives ("//line") can be used to bypass the restrictions on "//go:cgo_" directives, allowing blocked linker and compiler flags to be passed during compilation. This can result in unexpected execution of arbitrary code when running "go build". The line directive requires the absolute path of the file in which the directive lives, which makes exploiting this issue significantly more complex.	8.1	More Details
CVE-2023-22618	If Security Hardening guide rules are not followed, then Nokia WaveLite products allow a local user to create new users with administrative privileges by manipulating a web request. This affects (for example) WaveLite Metro 200 and Fan, WaveLite Metro 200 OPS and Fans, WaveLite Metro 200 and F2B fans, WaveLite Metro 200 OPS and F2B fans, WaveLite Metro 200 NE and F2B fans, and WaveLite Metro 200 NE OPS and F2B fans.	8.1	More Details
CVE-2023-41771	Layer 2 Tunneling Protocol Remote Code Execution Vulnerability	8.1	More Details
CVE-2023-41770	Layer 2 Tunneling Protocol Remote Code Execution Vulnerability	8.1	More Details
CVE-2023-40537	An authenticated user's session cookie may remain valid for a limited time after logging out from the BIG-IP Configuration utility on a multi-blade VIPRION platform. Note: Software versions which have reached End of Technical Support (EoTS) are not evaluated.	8.1	More Details
CVE-2023-41768	Layer 2 Tunneling Protocol Remote Code Execution Vulnerability	8.1	More Details
CVE-2023-41767	Layer 2 Tunneling Protocol Remote Code Execution Vulnerability	8.1	More Details
CVE-2023-41765	Layer 2 Tunneling Protocol Remote Code Execution Vulnerability	8.1	More Details

CVE Number	Description	Base Score	Reference
CVE-2023-36778	Microsoft Exchange Server Remote Code Execution Vulnerability	8.0	More Details
CVE-2023-36711	Windows Runtime C++ Template Library Elevation of Privilege Vulnerability	7.8	More Details
CVE-2023-36723	Windows Container Manager Service Elevation of Privilege Vulnerability	7.8	More Details
CVE-2023-36704	Windows Setup Files Cleanup Remote Code Execution Vulnerability	7.8	More Details
CVE-2023-36743	Win32k Elevation of Privilege Vulnerability	7.8	More Details
CVE-2023-36418	Azure RTOS GUIX Studio Remote Code Execution Vulnerability	7.8	More Details
CVE-2023-36712	Windows Kernel Elevation of Privilege Vulnerability	7.8	More Details
CVE-2023-36420	Microsoft ODBC Driver for SQL Server Remote Code Execution Vulnerability	7.8	More Details
CVE-2023-36701	Microsoft Resilient File System (ReFS) Elevation of Privilege Vulnerability	7.8	More Details
CVE-2023-36702	Microsoft DirectMusic Remote Code Execution Vulnerability	7.8	More Details
CVE-2023-36725	Windows Kernel Elevation of Privilege Vulnerability	7.8	More Details
CVE-2023-36436	Windows MSHTML Platform Remote Code Execution Vulnerability	7.8	More Details

CVE Number	Description	Base Score	Reference
CVE-2023-36737	Azure Network Watcher VM Agent Elevation of Privilege Vulnerability	7.8	More Details
CVE-2023-36417	Microsoft SQL OLE DB Remote Code Execution Vulnerability	7.8	More Details
CVE-2023-36710	Windows Media Foundation Core Remote Code Execution Vulnerability	7.8	More Details
CVE-2023-40634	In phasechecksercer, there is a possible missing permission check. This could lead to local escalation of privilege with no additional execution privileges needed	7.8	More Details
CVE-2023-42788	An improper neutralization of special elements used in an os command ('OS Command Injection') vulnerability [CWE-78] in FortiManager & FortiAnalyzer version 7.4.0, version 7.2.0 through 7.2.3, version 7.0.0 through 7.0.8, version 6.4.0 through 6.4.12 and version 6.2.0 through 6.2.11 may allow a local attacker with low privileges to execute unauthorized code via specifically crafted arguments to a CLI command	7.8	More Details
CVE-2023-36726	Windows Internet Key Exchange (IKE) Extension Elevation of Privilege Vulnerability	7.8	More Details
CVE-2023-5463	A vulnerability was found in XINJE XDPPro up to 3.7.17a. It has been rated as critical. Affected by this issue is some unknown functionality in the library cfgmgr32.dll. The manipulation leads to uncontrolled search path. An attack has to be approached locally. The exploit has been disclosed to the public and may be used. VDB-241586 is the identifier assigned to this vulnerability. NOTE: The vendor was contacted early about this disclosure but did not respond in any way.	7.8	More Details
CVE-2023-4401	Dell SmartFabric Storage Software v1.4 (and earlier) contains an OS Command Injection Vulnerability in the CLI use of the ‘more’ command. A local or remote authenticated attacker could potentially exploit this vulnerability, leading to the ability to gain root-level access.	7.8	More Details
CVE-2023-36729	Named Pipe File System Elevation of Privilege Vulnerability	7.8	More Details

CVE Number	Description	Base Score	Reference
CVE-2023-43068	Dell SmartFabric Storage Software v1.4 (and earlier) contains an OS Command Injection Vulnerability in the restricted shell in SSH. An authenticated remote attacker could potentially exploit this vulnerability, leading to execute arbitrary commands.	7.8	More Details
CVE-2023-43069	Dell SmartFabric Storage Software v1.4 (and earlier) contain(s) an OS Command Injection Vulnerability in the CLI. An authenticated local attacker could potentially exploit this vulnerability, leading to possible injection of parameters to curl or docker.	7.8	More Details
CVE-2023-36731	Win32k Elevation of Privilege Vulnerability	7.8	More Details
CVE-2023-36732	Win32k Elevation of Privilege Vulnerability	7.8	More Details
CVE-2023-36730	Microsoft ODBC Driver for SQL Server Remote Code Execution Vulnerability	7.8	More Details
CVE-2023-40635	In linkturbo, there is a possible missing permission check. This could lead to local escalation of privilege with no additional execution privileges needed	7.8	More Details
CVE-2023-44083	A vulnerability has been identified in Tecnomatix Plant Simulation V2201 (All versions < V2201.0009), Tecnomatix Plant Simulation V2302 (All versions < V2302.0003). The affected application contains an out of bounds write past the end of an allocated buffer while parsing a specially crafted SPP file. This could allow an attacker to execute code in the context of the current process.	7.8	More Details
CVE-2023-44086	A vulnerability has been identified in Tecnomatix Plant Simulation V2201 (All versions < V2201.0009), Tecnomatix Plant Simulation V2302 (All versions < V2302.0003). The affected applications contain an out of bounds read past the end of an allocated structure while parsing specially crafted SPP files. This could allow an attacker to execute code in the context of the current process.	7.8	More Details
CVE-2023-44081	A vulnerability has been identified in Tecnomatix Plant Simulation V2201 (All versions < V2201.0009), Tecnomatix Plant Simulation V2302 (All versions < V2302.0003). The affected application contains an out of bounds write past the end of an allocated buffer while parsing a specially crafted SPP 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-2023-44082	A vulnerability has been identified in Tecnomatix Plant Simulation V2201 (All versions < V2201.0009), Tecnomatix Plant Simulation V2302 (All versions < V2302.0003). The affected application contains an out of bounds write past the end of an allocated buffer while parsing a specially crafted SPP file. This could allow an attacker to execute code in the context of the current process.	7.8	More Details
CVE-2023-36598	Microsoft WDAC ODBC Driver Remote Code Execution Vulnerability	7.8	More Details
CVE-2023-44084	A vulnerability has been identified in Tecnomatix Plant Simulation V2201 (All versions < V2201.0009), Tecnomatix Plant Simulation V2302 (All versions < V2302.0003). The affected applications contain an out of bounds read past the end of an allocated structure while parsing specially crafted SPP files. This could allow an attacker to execute code in the context of the current process.	7.8	More Details
CVE-2023-36557	PrintHTML API Remote Code Execution Vulnerability	7.8	More Details
CVE-2023-41772	Win32k Elevation of Privilege Vulnerability	7.8	More Details
CVE-2023-2809	Plaintext credential usage vulnerability in Sage 200 Spain 2023.38.001 version, the exploitation of which could allow a remote attacker to extract SQL database credentials from the DLL application. This vulnerability could be linked to known techniques to obtain remote execution of MS SQL commands and escalate privileges on Windows systems because the credentials are stored in plaintext.	7.8	More Details
CVE-2023-44085	A vulnerability has been identified in Tecnomatix Plant Simulation V2201 (All versions < V2201.0009), Tecnomatix Plant Simulation V2302 (All versions < V2302.0003). The affected applications contain an out of bounds read past the end of an allocated structure while parsing specially crafted SPP files. This could allow an attacker to execute code in the context of the current process.	7.8	More Details
CVE-2023-44087	A vulnerability has been identified in Tecnomatix Plant Simulation V2201 (All versions < V2201.0009), Tecnomatix Plant Simulation V2302 (All versions < V2302.0003). The affected applications contain an out of bounds read past the end of an allocated structure while parsing specially crafted SPP files. 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-2023-41766	Windows Client Server Run-time Subsystem (CSRSS) Elevation of Privilege Vulnerability	7.8	More Details
CVE-2023-45204	A vulnerability has been identified in Tecnomatix Plant Simulation V2201 (All versions < V2201.0009), Tecnomatix Plant Simulation V2302 (All versions < V2302.0003). The affected applications contain a type confusion vulnerability while parsing specially crafted IGS files. This could allow an attacker to execute code in the context of the current process. (ZDI-CAN-21268)	7.8	More Details
CVE-2023-45205	A vulnerability has been identified in SICAM PAS/PQS (All versions >= V8.00 < V8.20). The affected application is installed with specific files and folders with insecure permissions. This could allow an authenticated local attacker to inject arbitrary code and escalate privileges to `NT AUTHORITY/SYSTEM`.	7.8	More Details
CVE-2023-45601	A vulnerability has been identified in Parasolid V35.0 (All versions < V35.0.262), Parasolid V35.1 (All versions < V35.1.250), Parasolid V36.0 (All versions < V36.0.169), Tecnomatix Plant Simulation V2201 (All versions < V2201.0009), Tecnomatix Plant Simulation V2302 (All versions < V2302.0003). The affected applications contain a stack overflow vulnerability while parsing specially crafted IGS files. This could allow an attacker to execute code in the context of the current process. (ZDI-CAN-21290)	7.8	More Details
CVE-2023-31096	An issue was discovered in Broadcom) LSI PCI-SV92EX Soft Modem Kernel Driver through 2.2.100.1 (aka AGRSM64.sys). There is Local Privilege Escalation to SYSTEM via a Stack Overflow in RTLCopyMemory (IOCTL 0x1b2150). An attacker can exploit this to elevate privileges from a medium-integrity process to SYSTEM. This can also be used to bypass kernel-level protections such as AV or PPL, because exploit code runs with high-integrity privileges and can be used in coordinated BYOVD (bring your own vulnerable driver) ransomware campaigns.	7.8	More Details
CVE-2023-30733	Stack-based Buffer Overflow in vulnerability HDCP trustlet prior to SMR Oct-2023 Release 1 allows local privileged attackers to perform code execution.	7.8	More Details
CVE-2023-43611	The BIG-IP Edge Client Installer on macOS does not follow best practices for elevating privileges during the installation process. This vulnerability is due to an incomplete fix for CVE-2023-38418. Note: Software versions which have reached End of Technical Support (EoTS) are not evaluated	7.8	More Details

CVE Number	Description	Base Score	Reference
CVE-2023-43787	A vulnerability was found in libX11 due to an integer overflow within the XCreateImage() function. This flaw allows a local user to trigger an integer overflow and execute arbitrary code with elevated privileges.	7.8	More Details
CVE-2023-21266	In multiple functions of ActivityManagerService.java, there is a possible way to escape Google Play protection due to a permissions bypass. This could lead to local escalation of privilege with no additional execution privileges needed. User interaction is not needed for exploitation.	7.8	More Details
CVE-2023-30900	A vulnerability has been identified in Xpedition Layout Browser (All versions < VX.2.14). Affected application contains a stack overflow vulnerability when parsing a PCB file. An attacker can leverage this vulnerability to execute code in the context of the current process.	7.8	More Details
CVE-2023-36718	Microsoft Virtual Trusted Platform Module Remote Code Execution Vulnerability	7.8	More Details
CVE-2023-36785	Microsoft ODBC Driver for SQL Server Remote Code Execution Vulnerability	7.8	More Details
CVE-2023-44209	Local privilege escalation due to improper soft link handling. The following products are affected: Acronis Agent (Linux, macOS, Windows) before build 29051.	7.8	More Details
CVE-2023-43896	A buffer overflow in Macrium Reflect 8.1.7544 and below allows attackers to escalate privileges or execute arbitrary code.	7.8	More Details
CVE-2023-40299	Kong Insomnia 2023.4.0 on macOS allows attackers to execute code and access restricted files, or make requests for TCC permissions, by using the DYLD_INSERT_LIBRARIES environment variable.	7.8	More Details
CVE-2023-25607	An improper neutralization of special elements used in an OS Command ('OS Command Injection') vulnerability [CWE-78] in FortiManager 7.2.0 through 7.2.2, 7.0.0 through 7.0.7, 6.4.0 through 6.4.11, 6.2 all versions, 6.0 all versions, FortiAnalyzer 7.2.0 through 7.2.2, 7.0.0 through 7.0.7, 6.4.0 through 6.4.11, 6.2 all versions, 6.0 all versions and FortiADC 7.1.0, 7.0.0 through 7.0.3, 6.2 all versions, 6.1 all versions, 6.0 all versions management interface may allow an authenticated attacker with at least READ permissions on system settings to execute arbitrary commands on the underlying shell due to an unsafe usage of the wordexp function.	7.8	More Details

CVE Number	Description	Base Score	Reference
CVE-2023-43838	An arbitrary file upload vulnerability in Personal Management System v1.4.64 allows attackers to execute arbitrary code via uploading a crafted SVG file into a user profile's avatar.	7.8	More Details
CVE-2023-36790	Windows RDP Encoder Mirror Driver Elevation of Privilege Vulnerability	7.8	More Details
CVE-2023-36123	Directory Traversal vulnerability in Hex-Dragon Plain Craft Launcher 2 version Alpha 1.3.9, allows local attackers to execute arbitrary code and gain sensitive information.	7.8	More Details
CVE-2022-30527	A vulnerability has been identified in SINEC NMS (All versions < V2.0). The affected application assigns improper access rights to specific folders containing executable files and libraries. This could allow an authenticated local attacker to inject arbitrary code and escalate privileges.	7.8	More Details
CVE-2023-42824	The issue was addressed with improved checks. This issue is fixed in iOS 16.7.1 and iPadOS 16.7.1. 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 16.6.	7.8	More Details
CVE-2023-36594	Windows Graphics Component Elevation of Privilege Vulnerability	7.8	More Details
CVE-2023-26236	An issue was discovered in WatchGuard EPDR 8.0.21.0002. Due to a weak implementation of message handling between WatchGuard EPDR processes, it is possible to perform a Local Privilege Escalation on Windows by sending a crafted message to a named pipe.	7.8	More Details
CVE-2023-36593	Microsoft Message Queuing (MSMQ) Remote Code Execution Vulnerability	7.8	More Details
CVE-2023-43700	Missing Authorization in RDT400 in SICK APU allows an unprivileged remote attacker to modify data via HTTP requests that no not require authentication.	7.7	More Details
CVE-2023-23366	A path traversal vulnerability has been reported to affect Music Station. If exploited, the vulnerability could allow authenticated users to read the contents of unexpected files and expose sensitive data via a network. We have already fixed the vulnerability in the following version: Music Station 5.3.22 and later	7.7	More Details

CVE Number	Description	Base Score	Reference
CVE-2023-23365	A path traversal vulnerability has been reported to affect Music Station. If exploited, the vulnerability could allow authenticated users to read the contents of unexpected files and expose sensitive data via a network. We have already fixed the vulnerability in the following version: Music Station 5.3.22 and later	7.7	More Details
CVE-2023-3361	A flaw was found in Red Hat OpenShift Data Science. When exporting a pipeline from the Elyra notebook pipeline editor as Python DSL or YAML, it reads S3 credentials from the cluster (ds pipeline server) and saves them in plain text in the generated output instead of an ID for a Kubernetes secret.	7.7	More Details
CVE-2023-3725	Potential buffer overflow vulnerability in the Zephyr CAN bus subsystem	7.6	More Details
CVE-2023-43810	OpenTelemetry, also known as OTel for short, is a vendor-neutral open-source Observability framework for instrumenting, generating, collecting, and exporting telemetry data such as traces, metrics, logs. Autoinstrumentation out of the box adds the label `http_method` that has unbound cardinality. It leads to the server's potential memory exhaustion when many malicious requests are sent. HTTP method for requests can be easily set by an attacker to be random and long. In order to be affected program has to be instrumented for HTTP handlers and does not filter any unknown HTTP methods on the level of CDN, LB, previous middleware, etc. This issue has been patched in version 0.41b0.	7.5	More Details
CVE-2023-36596	Remote Procedure Call Information Disclosure Vulnerability	7.5	More Details
CVE-2023-45371	An issue was discovered in the Wikibase extension for MediaWiki before 1.35.12, 1.36.x through 1.39.x before 1.39.5, and 1.40.x before 1.40.1. There is no rate limit for merging items.	7.5	More Details
CVE-2023-36603	Windows TCP/IP Denial of Service Vulnerability	7.5	More Details
CVE-2023-36579	Microsoft Message Queuing (MSMQ) Denial of Service Vulnerability	7.5	More Details
CVE-2023-36567	Windows Deployment Services Information Disclosure Vulnerability	7.5	More Details

CVE Number	Description	Base Score	Reference
CVE-2023-36585	Windows upnphost.dll Denial of Service Vulnerability	7.5	More Details
CVE-2023-45363	An issue was discovered in ApiPageSet.php in MediaWiki before 1.35.12, 1.36.x through 1.39.x before 1.39.5, and 1.40.x before 1.40.1. It allows attackers to cause a denial of service (unbounded loop and RequestTimeoutException) when querying pages redirected to other variants with redirects and converttitles set.	7.5	More Details
CVE-2023-36581	Microsoft Message Queuing (MSMQ) Denial of Service Vulnerability	7.5	More Details
CVE-2023-36606	Microsoft Message Queuing (MSMQ) Denial of Service Vulnerability	7.5	More Details
CVE-2023-36435	Microsoft QUIC Denial of Service Vulnerability	7.5	More Details
CVE-2023-36709	Microsoft AllJoyn API Denial of Service Vulnerability	7.5	More Details
CVE-2023-36703	DHCP Server Service Denial of Service Vulnerability	7.5	More Details
CVE-2023-44860	An issue in NETIS SYSTEMS N3Mv2 v.1.0.1.865 allows a remote attacker to cause a denial of service via the authorization component in the HTTP request.	7.5	More Details
CVE-2023-36438	Windows TCP/IP Information Disclosure Vulnerability	7.5	More Details
CVE-2023-36431	Microsoft Message Queuing (MSMQ) Denial of Service Vulnerability	7.5	More Details
CVE-2023-36602	Windows TCP/IP Denial of Service Vulnerability	7.5	More Details

CVE Number	Description	Base Score	Reference
CVE-2023-44839	D-Link DIR-823G A1V1.0.2B05 was discovered to contain a buffer overflow via the Encryption parameter in the SetWLanRadioSecurity function. This vulnerability allows attackers to cause a Denial of Service (DoS) via a crafted input.	7.5	More Details
CVE-2023-43699	Improper Restriction of Excessive Authentication Attempts in RDT400 in SICK APU allows an unprivileged remote attacker to guess the password via trial-and-error as the login attempts are not limited.	7.5	More Details
CVE-2023-3512	Relative path traversal vulnerability in Setelsa Security's ConacWin CB, in its 3.8.2.2 version and earlier, the exploitation of which could allow an attacker to perform an arbitrary download of files from the system via the "Download file" parameter.	7.5	More Details
CVE-2023-36720	Windows Mixed Reality Developer Tools Denial of Service Vulnerability	7.5	More Details
CVE-2023-43793	Misskey is an open source, decentralized social media platform. Prior to version 2023.9.0, by editing the URL, a user can bypass the authentication of the Bull dashboard, which is the job queue management UI, and access it. Version 2023.9.0 contains a fix. There are no known workarounds.	7.5	More Details
CVE-2023-42189	Insecure Permissions vulnerability in Connectivity Standards Alliance Matter Official SDK v.1.1.0.0 , Nanoleaf Light strip v.3.5.10, Govee LED Strip v.3.00.42, switchBot Hub2 v.1.0-0.8, Phillips hue hub v.1.59.1959097030, and yeelight smart lamp v.1.12.69 allows a remote attacker to cause a denial of service via a crafted script to the KeySetRemove function.	7.5	More Details
CVE-2020-27213	An issue was discovered in Ethernut Nut/OS 5.1. The code that generates Initial Sequence Numbers (ISNs) for TCP connections derives the ISN from an insufficiently random source. As a result, an attacker may be able to determine the ISN of current and future TCP connections and either hijack existing ones or spoof future ones. While the ISN generator seems to adhere to RFC 793 (where a global 32-bit counter is incremented roughly every 4 microseconds), proper ISN generation should aim to follow at least the specifications outlined in RFC 6528.	7.5	More Details
CVE-2023-38171	Microsoft QUIC Denial of Service Vulnerability	7.5	More Details

CVE Number	Description	Base Score	Reference
CVE-2023-42796	A vulnerability has been identified in CP-8031 MASTER MODULE (All versions < CPCI85 V05.11), CP-8050 MASTER MODULE (All versions < CPCI85 V05.11). The web server of affected devices fails to properly sanitize user input for the /sicweb-ajax/tmproot/ endpoint. This could allow an authenticated remote attacker to traverse directories on the system and download arbitrary files. By exploring active session IDs, the vulnerability could potentially be leveraged to escalate privileges to the administrator role.	7.5	More Details
CVE-2023-43261	An information disclosure in Milesight UR5X, UR32L, UR32, UR35, UR41 before v35.3.0.7 allows attackers to access sensitive router components.	7.5	More Details
CVE-2023-1584	A flaw was found in Quarkus. Quarkus OIDC can leak both ID and access tokens in the authorization code flow when an insecure HTTP protocol is used, which can allow attackers to access sensitive user data directly from the ID token or by using the access token to access user data from OIDC provider services. Please note that passwords are not stored in access tokens.	7.5	More Details
CVE-2023-36478	Eclipse Jetty provides a web server and servlet container. In versions 11.0.0 through 11.0.15, 10.0.0 through 10.0.15, and 9.0.0 through 9.4.52, an integer overflow in `MetaDataBuilder.checkSize` allows for HTTP/2 HPACK header values to exceed their size limit. `MetaDataBuilder.java` determines if a header name or value exceeds the size limit, and throws an exception if the limit is exceeded. However, when length is very large and huffman is true, the multiplication by 4 in line 295 will overflow, and length will become negative. `(_size+length)` will now be negative, and the check on line 296 will not be triggered. Furthermore, `MetaDataBuilder.checkSize` allows for user-entered HPACK header value sizes to be negative, potentially leading to a very large buffer allocation later on when the user-entered size is multiplied by 2. This means that if a user provides a negative length value (or, more precisely, a length value which, when multiplied by the 4/3 fudge factor, is negative), and this length value is a very large positive number when multiplied by 2, then the user can cause a very large buffer to be allocated on the server. Users of HTTP/2 can be impacted by a remote denial of service attack. The issue has been fixed in versions 11.0.16, 10.0.16, and 9.4.53. There are no known workarounds.	7.5	More Details
CVE-2023-5499	Information exposure vulnerability in Shenzhen Reachfar v28, the exploitation of which could allow a remote attacker to retrieve all the week's logs stored in the 'log2' directory. An attacker could retrieve sensitive information such as remembered wifi networks, sent messages, SOS device locations and device configurations.	7.5	More Details

CVE Number	Description	Base Score	Reference
CVE-2023-40534	When a client-side HTTP/2 profile and the HTTP MRF Router option are enabled for a virtual server, and an iRule using the HTTP_REQUEST event or Local Traffic Policy are associated with the virtual server, undisclosed requests can cause TMM to terminate. Note: Software versions which have reached End of Technical Support (EoTS) are not evaluated.	7.5	More Details
CVE-2023-40542	When TCP Verified Accept is enabled on a TCP profile that is configured on a Virtual Server, undisclosed requests can cause an increase in memory resource utilization. Note: Software versions which have reached End of Technical Support (EoTS) are not evaluated	7.5	More Details
CVE-2023-41085	When IPSec is configured on a Virtual Server, undisclosed traffic can cause TMM to terminate. Note: Software versions which have reached End of Technical Support (EoTS) are not evaluated.	7.5	More Details
CVE-2023-45349	Atos Unify OpenScape 4000 Assistant V10 R1 before V10 R1.34.7, 4000 Assistant V10 R1.42.0, 4000 Assistant V10 R0, 4000 Manager V10 R1 before V10 R1.34.7, 4000 Manager V10 R1.42.0, and 4000 Manager V10 R0 expose sensitive information that may allow lateral movement to the backup system via AShbr. This is also known as OSFOURK-23722.	7.5	More Details
CVE-2023-44487	The HTTP/2 protocol allows a denial of service (server resource consumption) because request cancellation can reset many streams quickly, as exploited in the wild in August through October 2023.	7.5	More Details
CVE-2023-36127	User enumeration is found in in PHPJabbers Appointment Scheduler 3.0. This issue occurs during password recovery, where a difference in messages could allow an attacker to determine if the user is valid or not, enabling a brute force attack with valid users.	7.5	More Details

CVE Number	Description	Base Score	Reference
CVE-2023-43809	Soft Serve is a self-hostable Git server for the command line. Prior to version 0.6.2, a security vulnerability in Soft Serve could allow an unauthenticated, remote attacker to bypass public key authentication when keyboard-interactive SSH authentication is active, through the `allow-keyless` setting, and the public key requires additional client-side verification for example using FIDO2 or GPG. This is due to insufficient validation procedures of the public key step during SSH request handshake, granting unauthorized access if the keyboard-interaction mode is utilized. An attacker could exploit this vulnerability by presenting manipulated SSH requests using keyboard-interactive authentication mode. This could potentially result in unauthorized access to the Soft Serve. Users should upgrade to the latest Soft Serve version `v0.6.2` to receive the patch for this issue. To workaround this vulnerability without upgrading, users can temporarily disable Keyboard-Interactive SSH Authentication using the `allow-keyless` setting.	7.5	More Details
CVE-2023-43805	Nexkey is a fork of Misskey, an open source, decentralized social media platform. Prior to version 12.121.9, incomplete URL validation can allow users to bypass authentication for access to the job queue dashboard. Version 12.121.9 contains a fix for this issue. As a workaround, it may be possible to avoid this by blocking access using tools such as Cloudflare's WAF.	7.5	More Details
CVE-2023-44834	D-Link DIR-823G A1V1.0.2B05 was discovered to contain a buffer overflow via the StartTime parameter in the SetParentsControlInfo function. This vulnerability allows attackers to cause a Denial of Service (DoS) via a crafted input.	7.5	More Details
CVE-2023-45198	ftpd before "NetBSD-ftpd 20230930" can leak information about the host filesystem before authentication via an MLSD or MLST command. tnftpd (the portable version of NetBSD ftpd) before 20231001 is also vulnerable.	7.5	More Details
CVE-2023-43615	Mbed TLS 2.x before 2.28.5 and 3.x before 3.5.0 has a Buffer Overflow.	7.5	More Details
CVE-2023-40632	In jpg driver, there is a possible use after free due to a logic error. This could lead to remote information disclosure no additional execution privileges needed	7.5	More Details
CVE-2023-29348	Windows Remote Desktop Gateway (RD Gateway) Information Disclosure Vulnerability	7.5	More Details

CVE Number	Description	Base Score	Reference
CVE-2023-40718	A interpretation conflict in Fortinet IPS Engine versions 7.321, 7.166 and 6.158 allows attacker to evade IPS features via crafted TCP packets.	7.5	More Details
CVE-2023-44838	D-Link DIR-823G A1V1.0.2B05 was discovered to contain a buffer overflow via the TXPower parameter in the SetWLanRadioSettings function. This vulnerability allows attackers to cause a Denial of Service (DoS) via a crafted input.	7.5	More Details
CVE-2023-44837	D-Link DIR-823G A1V1.0.2B05 was discovered to contain a buffer overflow via the Password parameter in the SetWanSettings function. This vulnerability allows attackers to cause a Denial of Service (DoS) via a crafted input.	7.5	More Details
CVE-2023-44836	D-Link DIR-823G A1V1.0.2B05 was discovered to contain a buffer overflow via the SSID parameter in the SetWLanRadioSettings function. This vulnerability allows attackers to cause a Denial of Service (DoS) via a crafted input.	7.5	More Details
CVE-2023-44835	D-Link DIR-823G A1V1.0.2B05 was discovered to contain a buffer overflow via the Mac parameter in the SetParentsControlInfo function. This vulnerability allows attackers to cause a Denial of Service (DoS) via a crafted input.	7.5	More Details
CVE-2023-45282	In NASA Open MCT (aka openmct) before 3.1.0, prototype pollution can occur via an import action.	7.5	More Details
CVE-2023-44833	D-Link DIR-823G A1V1.0.2B05 was discovered to contain a buffer overflow via the GuardInt parameter in the SetWLanRadioSettings function. This vulnerability allows attackers to cause a Denial of Service (DoS) via a crafted input.	7.5	More Details
CVE-2023-44832	D-Link DIR-823G A1V1.0.2B05 was discovered to contain a buffer overflow via the MacAddress parameter in the SetWanSettings function. This vulnerability allows attackers to cause a Denial of Service (DoS) via a crafted input.	7.5	More Details
CVE-2023-44831	D-Link DIR-823G A1V1.0.2B05 was discovered to contain a buffer overflow via the Type parameter in the SetWLanRadioSettings function. This vulnerability allows attackers to cause a Denial of Service (DoS) via a crafted input.	7.5	More Details

CVE Number	Description	Base Score	Reference
CVE-2023-44830	D-Link DIR-823G A1V1.0.2B05 was discovered to contain a buffer overflow via the EndTime parameter in the SetParentsControlInfo function. This vulnerability allows attackers to cause a Denial of Service (DoS) via a crafted input.	7.5	More Details
CVE-2023-44829	D-Link DIR-823G A1V1.0.2B05 was discovered to contain a buffer overflow via the AdminPassword parameter in the SetDeviceSettings function. This vulnerability allows attackers to cause a Denial of Service (DoS) via a crafted input.	7.5	More Details
CVE-2023-44828	D-Link DIR-823G A1V1.0.2B05 was discovered to contain a buffer overflow via the CurrentPassword parameter in the CheckPasswdSettings function. This vulnerability allows attackers to cause a Denial of Service (DoS) via a crafted input.	7.5	More Details
CVE-2023-4586	A vulnerability was found in the Hot Rod client. This security issue occurs as the Hot Rod client does not enable hostname validation when using TLS, possibly resulting in a man-in-the-middle (MITM) attack.	7.4	More Details
CVE-2023-36605	Windows Named Pipe Filesystem Elevation of Privilege Vulnerability	7.4	More Details
CVE-2020-18336	Cross Site Scripting (XSS) vulnerability found in Typora v.0.9.65 allows a remote attacker to obtain sensitive information via the PDF file exporting function.	7.4	More Details
CVE-2023-45226	The BIG-IP SPK TMM (Traffic Management Module) f5-debug-sidecar and f5-debug-sshd containers contains hardcoded credentials that may allow an attacker with the ability to intercept traffic to impersonate the SPK Secure Shell (SSH) server on those containers. This is only exposed when ssh debug is enabled. Note: Software versions which have reached End of Technical Support (EoTS) are not evaluated	7.4	More Details
CVE-2023-36574	Microsoft Message Queuing (MSMQ) Remote Code Execution Vulnerability	7.3	More Details
CVE-2023-36578	Microsoft Message Queuing (MSMQ) Remote Code Execution Vulnerability	7.3	More Details
CVE-2023-36575	Microsoft Message Queuing (MSMQ) Remote Code Execution Vulnerability	7.3	More Details

CVE Number	Description	Base Score	Reference
CVE-2023-5450	An insufficient verification of data vulnerability exists in BIG-IP Edge Client Installer on macOS that may allow an attacker elevation of privileges during the installation process. Note: Software versions which have reached End of Technical Support (EoTS) are not evaluated.	7.3	More Details
CVE-2023-36571	Microsoft Message Queuing (MSMQ) Remote Code Execution Vulnerability	7.3	More Details
CVE-2023-36592	Microsoft Message Queuing (MSMQ) Remote Code Execution Vulnerability	7.3	More Details
CVE-2023-5373	A vulnerability classified as critical has been found in SourceCodester Online Computer and Laptop Store 1.0. Affected is the function register of the file Master.php. The manipulation of the argument email leads to sql injection. It is possible to launch the attack remotely. The exploit has been disclosed to the public and may be used. VDB-241254 is the identifier assigned to this vulnerability.	7.3	More Details
CVE-2023-3971	An HTML injection flaw was found in Controller in the user interface settings. This flaw allows an attacker to capture credentials by creating a custom login page by injecting HTML, resulting in a complete compromise.	7.3	More Details
CVE-2023-4237	A flaw was found in the Ansible Automation Platform. When creating a new keypair, the ec2_key module prints out the private key directly to the standard output. This flaw allows an attacker to fetch those keys from the log files, compromising the system's confidentiality, integrity, and availability.	7.3	More Details
CVE-2023-36573	Microsoft Message Queuing (MSMQ) Remote Code Execution Vulnerability	7.3	More Details
CVE-2023-36570	Microsoft Message Queuing (MSMQ) Remote Code Execution Vulnerability	7.3	More Details
CVE-2023-45248	Local privilege escalation due to DLL hijacking vulnerability. The following products are affected: Acronis Cyber Protect Cloud Agent (Windows) before build 36497, Acronis Cyber Protect 16 (Windows) before build 37391.	7.3	More Details

CVE Number	Description	Base Score	Reference
CVE-2023-36572	Microsoft Message Queuing (MSMQ) Remote Code Execution Vulnerability	7.3	More Details
CVE-2023-36591	Microsoft Message Queuing (MSMQ) Remote Code Execution Vulnerability	7.3	More Details
CVE-2023-36590	Microsoft Message Queuing (MSMQ) Remote Code Execution Vulnerability	7.3	More Details
CVE-2023-36589	Microsoft Message Queuing (MSMQ) Remote Code Execution Vulnerability	7.3	More Details
CVE-2023-36583	Microsoft Message Queuing (MSMQ) Remote Code Execution Vulnerability	7.3	More Details
CVE-2023-36582	Microsoft Message Queuing (MSMQ) Remote Code Execution Vulnerability	7.3	More Details
CVE-2023-36561	Azure DevOps Server Elevation of Privilege Vulnerability	7.3	More Details
CVE-2023-44847	An issue in SeaCMS v.12.8 allows an attacker to execute arbitrary code via the admin_ Weixin.php component.	7.2	More Details
CVE-2023-36780	Skype for Business Remote Code Execution Vulnerability	7.2	More Details
CVE-2023-36786	Skype for Business Remote Code Execution Vulnerability	7.2	More Details
CVE-2023-36789	Skype for Business Remote Code Execution Vulnerability	7.2	More Details

CVE Number	Description	Base Score	Reference
CVE-2023-42768	When a non-admin user has been assigned an administrator role via an iControl REST PUT request and later the user's role is reverted back to a non-admin role via the Configuration utility, tmsh, or iControl REST. BIG-IP non-admin user can still have access to iControl REST admin resource. Note: Software versions which have reached End of Technical Support (EoTS) are not evaluated.	7.2	More Details
CVE-2023-45247	Sensitive information disclosure and manipulation due to missing authorization. The following products are affected: Acronis Cyber Protect Cloud Agent (Linux, macOS, Windows) before build 36497, Acronis Cyber Protect 16 (Linux, macOS, Windows) before build 39169.	7.1	More Details
CVE-2023-41838	An improper neutralization of special elements used in an os command ('os command injection') in FortiManager 7.4.0 and 7.2.0 through 7.2.3 may allow attacker to execute unauthorized code or commands via FortiManager cli.	7.1	More Details
CVE-2023-44378	gnark is a zk-SNARK library that offers a high-level API to design circuits. Prior to version 0.9.0, for some in-circuit values, it is possible to construct two valid decomposition to bits. In addition to the canonical decomposition of `a`, for small values there exists a second decomposition for `a+r` (where `r` is the modulus the values are being reduced by). The second decomposition was possible due to overflowing the field where the values are defined. Upgrading to version 0.9.0 should fix the issue without needing to change the calls to value comparison methods.	7.1	More Details
CVE-2023-43698	Improper Neutralization of Input During Web Page Generation (’Cross-site Scripting’) in RDT400 in SICK APU allows an unprivileged remote attacker to run arbitrary code in the clients browser via injecting code into the website.	7.1	More Details
CVE-2023-45244	Sensitive information disclosure and manipulation due to missing authorization. The following products are affected: Acronis Cyber Protect Cloud Agent (Linux, macOS, Windows) before build 35895, Acronis Cyber Protect 16 (Linux, macOS, Windows) before build 37391.	7.1	More Details
CVE-2023-44211	Sensitive information disclosure and manipulation due to missing authorization. The following products are affected: Acronis Cyber Protect Cloud Agent (Linux, macOS, Windows) before build 31637, Acronis Cyber Protect 16 (Linux, Windows) before build 37391.	7.1	More Details

CVE Number	Description	Base Score	Reference
CVE-2023-5369	Before correction, the copy_file_range system call checked only for the CAP_READ and CAP_WRITE capabilities on the input and output file descriptors, respectively. Using an offset is logically equivalent to seeking, and the system call must additionally require the CAP_SEEK capability. This incorrect privilege check enabled sandboxed processes with only read or write but no seek capability on a file descriptor to read data from or write data to an arbitrary location within the file corresponding to that file descriptor.	7.1	More Details
CVE-2023-45246	Sensitive information disclosure and manipulation due to missing authorization. The following products are affected: Acronis Cyber Protect Cloud Agent (Linux, macOS, Windows) before build 36343, Acronis Cyber Protect 16 (Linux, macOS, Windows) before build 39169.	7.1	More Details
CVE-2023-44212	Sensitive information disclosure and manipulation due to missing authorization. The following products are affected: Acronis Agent (Linux, macOS, Windows) before build 31477.	7.1	More Details
CVE-2023-5377	Out-of-bounds Read in GitHub repository gpac/gpac prior to v2.2.2-DEV.	7.1	More Details
CVE-2023-5366	A flaw was found in Open vSwitch that allows ICMPv6 Neighbor Advertisement packets between virtual machines to bypass OpenFlow rules. This issue may allow a local attacker to create specially crafted packets with a modified or spoofed target IP address field that can redirect ICMPv6 traffic to arbitrary IP addresses.	7.1	More Details
CVE-2023-36565	Microsoft Office Graphics Elevation of Privilege Vulnerability	7.0	More Details
CVE-2023-36568	Microsoft Office Click-To-Run Elevation of Privilege Vulnerability	7.0	More Details
CVE-2023-36902	Windows Runtime Remote Code Execution Vulnerability	7.0	More Details
CVE-2023-38159	Windows Graphics Component Elevation of Privilege Vulnerability	7.0	More Details

CVE Number	Description	Base Score	Reference
CVE-2023-36776	Win32k Elevation of Privilege Vulnerability	7.0	More Details
CVE-2023-36721	Windows Error Reporting Service Elevation of Privilege Vulnerability	7.0	More Details
CVE-2022-35950	OroCommerce is an open-source Business to Business Commerce application. In versions 4.1.0 through 4.1.13, 4.2.0 through 4.2.10, 5.0.0 prior to 5.0.11, and 5.1.0 prior to 5.1.1, the JS payload added to the product name may be executed at the storefront when adding a note to the shopping list line item containing a vulnerable product. An attacker should be able to edit a product in the admin area and force a user to add this product to Shopping List and click add a note for it. Versions 5.0.11 and 5.1.1 contain a fix for this issue.	6.9	More Details
CVE-2023-42474	SAP BusinessObjects Web Intelligence - version 420, has a URL with parameter that could be vulnerable to XSS attack. The attacker could send a malicious link to a user that would possibly allow an attacker to retrieve the sensitive information.	6.8	More Details
CVE-2023-3589	A Cross-Site Request Forgery (CSRF) vulnerability affecting Teamwork Cloud from No Magic Release 2021x through No Magic Release 2022x could allow with some very specific conditions an attacker to send a specifically crafted query to the server.	6.8	More Details
CVE-2023-1832	An improper access control flaw was found in Candlepin. An attacker can create data scoped under another customer/tenant, which can result in loss of confidentiality and availability for the affected customer/tenant.	6.8	More Details
CVE-2023-42445	Gradle is a build tool with a focus on build automation and support for multi-language development. In some cases, when Gradle parses XML files, resolving XML external entities is not disabled. Combined with an Out Of Band XXE attack (OOB-XXE), just parsing XML can lead to exfiltration of local text files to a remote server. Gradle parses XML files for several purposes. Most of the time, Gradle parses XML files it generated or were already present locally. Only Ivy XML descriptors and Maven POM files can be fetched from remote repositories and parsed by Gradle. In Gradle 7.6.3 and 8.4, resolving XML external entities has been disabled for all use cases to protect against this vulnerability. Gradle will now refuse to parse XML files that have XML external entities.	6.8	More Details
CVE-2023-45613	In JetBrains Ktor before 2.3.5 server certificates were not verified	6.8	More Details

CVE Number	Description	Base Score	Reference
CVE-2023-36697	Microsoft Message Queuing (MSMQ) Remote Code Execution Vulnerability	6.8	More Details
CVE-2023-30727	Improper access control vulnerability in SecSettings prior to SMR Oct-2023 Release 1 allows attackers to enable Wi-Fi and connect arbitrary Wi-Fi without User Interaction.	6.7	More Details
CVE-2023-40653	In FW-PackageManager, there is a possible missing permission check. This could lead to local escalation of privilege with System execution privileges needed	6.7	More Details
CVE-2022-3431	A potential vulnerability in a driver used during manufacturing process on some consumer Lenovo Notebook devices that was mistakenly not deactivated may allow an attacker with elevated privileges to modify secure boot setting by modifying an NVRAM variable.	6.7	More Details
CVE-2023-21244	In visitUris of Notification.java, there is a possible bypass of user profile boundaries due to a missing permission check. This could lead to local escalation of privilege with User execution privileges needed. User interaction is not needed for exploitation.	6.7	More Details
CVE-2023-44400	Uptime Kuma is a self-hosted monitoring tool. Prior to version 1.23.3, attackers with access to a user's device can gain persistent account access. This is caused by missing verification of Session Tokens after password changes and/or elapsed inactivity periods. Version 1.23.3 has a patch for the issue.	6.7	More Details
CVE-2022-22298	A improper neutralization of special elements used in an os command ('os command injection') in Fortinet FortiIsolator version 1.0.0, FortiIsolator version 1.1.0, FortiIsolator version 1.2.0 through 1.2.2, FortiIsolator version 2.0.0 through 2.0.1, FortiIsolator version 2.1.0 through 2.1.2, FortiIsolator version 2.2.0, FortiIsolator version 2.3.0 through 2.3.4 allows attacker to execute arbitrary OS commands in the underlying shell via specially crafted input parameters.	6.7	More Details
CVE-2023-37194	A vulnerability has been identified in SIMATIC CP 1604 (All versions), SIMATIC CP 1616 (All versions), SIMATIC CP 1623 (All versions), SIMATIC CP 1626 (All versions), SIMATIC CP 1628 (All versions). The kernel memory of affected devices is exposed to user-mode via direct memory access (DMA) which could allow a local attacker with administrative privileges to execute arbitrary code on the host system without any restrictions.	6.7	More Details

CVE Number	Description	Base Score	Reference
CVE-2023-26237	An issue was discovered in WatchGuard EPDR 8.0.21.0002. It is possible to bypass the defensive capabilities by adding a registry key as SYSTEM.	6.7	More Details
CVE-2023-39192	A flaw was found in the Netfilter subsystem in the Linux kernel. The xt_u32 module did not validate the fields in the xt_u32 structure. This flaw allows a local privileged attacker to trigger an out-of-bounds read by setting the size fields with a value beyond the array boundaries, leading to a crash or information disclosure.	6.7	More Details
CVE-2023-23370	An insufficiently protected credentials vulnerability has been reported to affect QVPN Device Client. If exploited, the vulnerability could allow local authenticated administrators to gain access to user accounts and access sensitive data used by the user account via unspecified vectors. We have already fixed the vulnerability in the following version: QVPN Windows 2.1.0.0518 and later	6.7	More Details
CVE-2023-40654	In FW-PackageManager, there is a possible missing permission check. This could lead to local escalation of privilege with System execution privileges needed	6.7	More Details
CVE-2023-38640	A vulnerability has been identified in SICAM PAS/PQS (All versions >= V8.00 < V8.22). The affected application is installed with specific files and folders with insecure permissions. This could allow an authenticated local attacker to read and modify configuration data in the context of the application process.	6.6	More Details
CVE-2023-42787	A client-side enforcement of server-side security [CWE-602] vulnerability in Fortinet FortiManager version 7.4.0 and before 7.2.3 and FortiAnalyzer version 7.4.0 and before 7.2.3 may allow a remote attacker with low privileges to access a privileged web console via client side code execution.	6.5	More Details
CVE-2023-41175	A vulnerability was found in libtiff due to multiple potential integer overflows in raw2tiff.c. This flaw allows remote attackers to cause a denial of service or possibly execute an arbitrary code via a crafted tiff image, which triggers a heap-based buffer overflow.	6.5	More Details
CVE-2023-41660	Cross-Site Request Forgery (CSRF) vulnerability in WPSynchro WP Synchro plugin <= 1.9.1 versions.	6.5	More Details
CVE-2023-43697	Modification of Assumed-Immutable Data (MAID) in RDT400 in SICK APU allows an unprivileged remote attacker to make the site unable to load necessary strings via changing file paths using HTTP requests.	6.5	More Details

CVE Number	Description	Base Score	Reference
CVE-2023-42477	SAP NetWeaver AS Java (GRMG Heartbeat application) - version 7.50, allows an attacker to send a crafted request from a vulnerable web application, causing limited impact on confidentiality and integrity of the application.	6.5	More Details
CVE-2023-37935	A use of GET request method with sensitive query strings vulnerability in Fortinet FortiOS 7.0.0 - 7.0.12, 7.2.0 - 7.2.5 and 7.4.0 allows an attacker to view plaintext passwords of remote services such as RDP or VNC, if the attacker is able to read the GET requests to those services.	6.5	More Details
CVE-2023-40310	SAP PowerDesigner Client - version 16.7, does not sufficiently validate BPMN2 XML document imported from an untrusted source. As a result, URLs of external entities in BPMN2 file, although not used, would be accessed during import. A successful attack could impact availability of SAP PowerDesigner Client.	6.5	More Details
CVE-2023-40745	LibTIFF is vulnerable to an integer overflow. This flaw allows remote attackers to cause a denial of service (application crash) or possibly execute an arbitrary code via a crafted tiff image, which triggers a heap-based buffer overflow.	6.5	More Details
CVE-2023-5462	A vulnerability was found in XINJE XD5E-30R-E 3.5.3b. It has been declared as critical. Affected by this vulnerability is an unknown functionality of the component Modbus Handler. The manipulation leads to denial of service. The exploit has been disclosed to the public and may be used. The identifier VDB-241585 was assigned to this vulnerability. NOTE: The vendor was contacted early about this disclosure but did not respond in any way.	6.5	More Details
CVE-2023-36717	Windows Virtual Trusted Platform Module Denial of Service Vulnerability	6.5	More Details
CVE-2022-36228	Nokelock Smart padlock O1 Version 5.3.0 is vulnerable to Insecure Permissions. By sending a request, you can add any device and set the device password in the Nokelock app.	6.5	More Details
CVE-2023-36429	Microsoft Dynamics 365 (On-Premises) Information Disclosure Vulnerability	6.5	More Details
CVE-2023-5368	On an msdosfs filesystem, the 'truncate' or 'ftruncate' system calls under certain circumstances populate the additional space in the file with unallocated data from the underlying disk device, rather than zero bytes. This may permit a user with write access to files on a msdosfs filesystem to read unintended data (e.g. from a previously deleted file).	6.5	More Details

CVE Number	Description	Base Score	Reference
CVE-2023-43785	A vulnerability was found in libX11 due to a boundary condition within the _XkbReadKeySyms() function. This flaw allows a local user to trigger an out-of-bounds read error and read the contents of memory on the system.	6.5	More Details
CVE-2023-33301	An improper access control vulnerability in Fortinet FortiOS 7.2.0 - 7.2.4 and 7.4.0 allows an attacker to access a restricted resource from a non trusted host.	6.5	More Details
CVE-2022-36277	The 'sReferencia', 'sDescripcion', 'txtCodigo' and 'txtDescripcion' parameters, in the frmGestionStock.aspx and frmEditServicio.aspx files in TCMAN GIM v8.0.1, could allow an attacker to perform persistent XSS attacks.	6.5	More Details
CVE-2023-20235	A vulnerability in the on-device application development workflow feature for the Cisco IOx application hosting infrastructure in Cisco IOS XE Software could allow an authenticated, remote attacker to access the underlying operating system as the root user. This vulnerability exists because Docker containers with the privileged runtime option are not blocked when they are in application development mode. An attacker could exploit this vulnerability by using the Docker CLI to access an affected device. The application development workflow is meant to be used only on development systems and not in production systems.	6.5	More Details
CVE-2023-45322	libxml2 through 2.11.5 has a use-after-free that can only occur after a certain memory allocation fails. This occurs in xmlUnlinkNode in tree.c. NOTE: the vendor's position is "I don't think these issues are critical enough to warrant a CVE ID ... because an attacker typically can't control when memory allocations fail."	6.5	More Details
CVE-2023-36707	Windows Deployment Services Denial of Service Vulnerability	6.5	More Details
CVE-2023-45367	An issue was discovered in the CheckUser extension for MediaWiki before 1.35.12, 1.36.x through 1.39.x before 1.39.5, and 1.40.x before 1.40.1. A user can use a rest.php/checkuser/v0/useragent-clienthints/revision/ URL to store an arbitrary number of rows in cu_useragent_clienthints, leading to a denial of service.	6.5	More Details
CVE-2023-42755	A flaw was found in the IPv4 Resource Reservation Protocol (RSVP) classifier in the Linux kernel. The xprt pointer may go beyond the linear part of the skb, leading to an out-of-bounds read in the `rsvp_classify` function. This issue may allow a local user to crash the system and cause a denial of service.	6.5	More Details

CVE Number	Description	Base Score	Reference
CVE-2023-5459	A vulnerability has been found in Delta Electronics DVP32ES2 PLC 1.48 and classified as critical. This vulnerability affects unknown code of the component Password Transmission Handler. The manipulation leads to denial of service. The exploit has been disclosed to the public and may be used. VDB-241582 is the identifier assigned to this vulnerability. NOTE: The vendor was contacted early about this disclosure but did not respond in any way.	6.5	More Details
CVE-2023-36433	Microsoft Dynamics 365 (On-Premises) Information Disclosure Vulnerability	6.5	More Details
CVE-2023-39854	The web interface of ATX Ucrypt through 3.5 allows authenticated users (or attackers using default credentials for the admin, master, or user account) to include files via a URL in the /hydra/view/get_cc_url url parameter. There can be resultant SSRF.	6.5	More Details
CVE-2023-36566	Microsoft Common Data Model SDK Denial of Service Vulnerability	6.5	More Details
CVE-2023-36564	Windows Search Security Feature Bypass Vulnerability	6.5	More Details
CVE-2023-36563	Microsoft WordPad Information Disclosure Vulnerability	6.5	More Details
CVE-2023-5214	In Puppet Bolt versions prior to 3.27.4, a path to escalate privileges was identified.	6.5	More Details
CVE-2023-36706	Windows Deployment Services Information Disclosure Vulnerability	6.5	More Details
CVE-2023-37404	IBM Observability with Instana 1.0.243 through 1.0.254 could allow an attacker on the network to execute arbitrary code on the host after a successful DNS poisoning attack. IBM X-Force ID: 259789.	6.4	More Details

CVE Number	Description	Base Score	Reference
CVE-2023-5291	The Blog Filter plugin for WordPress is vulnerable to Stored Cross-Site Scripting via 'AWL-BlogFilter' shortcode in versions up to, and including, 1.5.3 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-2023-5357	The Instagram for WordPress plugin for WordPress is vulnerable to Stored Cross-Site Scripting via shortcodes in versions up to, and including, 2.1.6 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-2023-5467	The GEO my WordPress plugin for WordPress is vulnerable to Stored Cross-Site Scripting via shortcodes in versions up to, and including, 4.0 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-2023-5468	The Slick Contact Forms plugin for WordPress is vulnerable to Stored Cross-Site Scripting via 'dcscf-link' shortcode in versions up to, and including, 1.3.7 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-2023-4380	A logic flaw exists in Ansible Automation platform. Whenever a private project is created with incorrect credentials, they are logged in plaintext. This flaw allows an attacker to retrieve the credentials from the log, resulting in the loss of confidentiality, integrity, and availability.	6.3	More Details
CVE-2023-5471	A vulnerability, which was classified as critical, was found in codeprojects Farmacia 1.0. Affected is an unknown function of the file index.php. The manipulation of the argument usario/senha leads to sql injection. 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-241608.	6.3	More Details

CVE Number	Description	Base Score	Reference
CVE-2023-5494	A vulnerability was found in Byzoro Smart S45F Multi-Service Secure Gateway Intelligent Management Platform up to 20230928 and classified as critical. Affected by this issue is some unknown functionality of the file /log/download.php. The manipulation of the argument file leads to os command injection. The attack may be launched remotely. The exploit has been disclosed to the public and may be used. VDB-241646 is the identifier assigned to this vulnerability. NOTE: The vendor was contacted early about this disclosure but did not respond in any way.	6.3	More Details
CVE-2023-5490	A vulnerability classified as critical was found in Byzoro Smart S45F Multi-Service Secure Gateway Intelligent Management Platform up to 20230928. This vulnerability affects unknown code of the file /useratte/userattestation.php. The manipulation of the argument web_img leads to unrestricted upload. The attack can be initiated remotely. The exploit has been disclosed to the public and may be used. VDB-241642 is the identifier assigned to this vulnerability. NOTE: The vendor was contacted early about this disclosure but did not respond in any way.	6.3	More Details
CVE-2023-5493	A vulnerability has been found in Byzoro Smart S45F Multi-Service Secure Gateway Intelligent Management Platform up to 20230928 and classified as critical. Affected by this vulnerability is an unknown functionality of the file /useratte/web.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-241645 was assigned to this vulnerability. NOTE: The vendor was contacted early about this disclosure but did not respond in any way.	6.3	More Details
CVE-2023-5491	A vulnerability, which was classified as critical, has been found in Byzoro Smart S45F Multi-Service Secure Gateway Intelligent Management Platform up to 20230928. This issue affects some unknown processing of the file /sysmanage/updatelib.php. The manipulation of the argument file_upload leads to unrestricted upload. 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-241643. NOTE: The vendor was contacted early about this disclosure but did not respond in any way.	6.3	More Details
CVE-2023-43070	Dell SmartFabric Storage Software v1.4 (and earlier) contains a Path Traversal Vulnerability in the HTTP interface. A remote authenticated attacker could potentially exploit this vulnerability, leading to modify or write arbitrary files to arbitrary locations in the license container.	6.3	More Details

CVE Number	Description	Base Score	Reference
CVE-2023-5374	A vulnerability classified as critical was found in SourceCodester Online Computer and Laptop Store 1.0. Affected by this vulnerability is an unknown functionality of the file products.php. The manipulation of the argument c 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-241255.	6.3	More Details
CVE-2023-5492	A vulnerability, which was classified as critical, was found in Byzoro Smart S45F Multi-Service Secure Gateway Intelligent Management Platform up to 20230928. Affected is an unknown function of the file /sysmanage/licence.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-241644. NOTE: The vendor was contacted early about this disclosure but did not respond in any way.	6.3	More Details
CVE-2015-10126	A vulnerability classified as critical was found in Easy2Map Photos Plugin 1.0.1 on WordPress. This vulnerability affects unknown code. The manipulation leads to sql injection. The attack can be initiated remotely. Upgrading to version 1.1.0 is able to address this issue. The patch is identified as 503d9ee2482d27c065f78d9546f076a406189908. It is recommended to upgrade the affected component. VDB-241318 is the identifier assigned to this vulnerability.	6.3	More Details
CVE-2023-5497	A vulnerability classified as critical has been found in Tongda OA 2017 11.10. Affected is an unknown function of the file general/hr/salary/welfare_manage/delete.php. The manipulation of the argument WELFARE_ID leads to sql injection. It is possible to launch the attack remotely. The exploit has been disclosed to the public and may be used. VDB-241650 is the identifier assigned to this vulnerability.	6.3	More Details
CVE-2023-5489	A vulnerability classified as critical has been found in Byzoro Smart S45F Multi-Service Secure Gateway Intelligent Management Platform up to 20230928. This affects an unknown part of the file /Tool/uploadfile.php. The manipulation of the argument 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 identifier VDB-241641 was assigned to this vulnerability. NOTE: The vendor was contacted early about this disclosure but did not respond in any way.	6.3	More Details
CVE-2023-25788	Cross-Site Request Forgery (CSRF) vulnerability in Saphali Saphali Woocommerce Lite plugin <= 1.8.13 versions.	6.3	More Details

CVE Number	Description	Base Score	Reference
CVE-2023-25822	ReportPortal is an AI-powered test automation platform. Prior to version 5.10.0 of the `com.epam.reportportal:service-api` module, corresponding to ReportPortal version 23.2, the ReportPortal database becomes unstable and reporting almost fully stops except for small launches with approximately 1 test inside when the test_item.path field is exceeded the allowable `ltree` field type indexing limit (path length>=120, approximately recursive nesting of the nested steps). REINDEX INDEX path_gist_idx and path_idx aren't helped. The problem was fixed in `com.epam.reportportal:service-api` module version 5.10.0 (product release 23.2), where the maximum number of nested elements were programmatically limited. A workaround is available. After deletion of the data with long paths, and reindexing both indexes (path_gist_idx and path_idx), the database becomes stable and ReportPortal works properly.	6.3	More Details
CVE-2023-5488	A vulnerability was found in Byzoro Smart S45F Multi-Service Secure Gateway Intelligent Management Platform up to 20230928. It has been rated 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. The identifier of this vulnerability is VDB-241640. NOTE: The vendor was contacted early about this disclosure but did not respond in any way.	6.3	More Details
CVE-2023-5495	A vulnerability was found in QDocs Smart School 6.4.1. It has been classified as critical. This affects an unknown part of the file /course/filterRecords/ of the component HTTP POST Request Handler. The manipulation of the argument searchdata[0][title]/searchdata[0][searchfield]/searchdata[0][searchvalue] leads to sql injection. It is possible to initiate the attack remotely. The associated identifier of this vulnerability is VDB-241647. NOTE: The vendor was contacted early about this disclosure but did not respond in any way.	6.3	More Details
CVE-2023-3428	A heap-based buffer overflow vulnerability was found in coders/tiff.c in ImageMagick. This issue may allow a local attacker to trick the user into opening a specially crafted file, resulting in an application crash and denial of service.	6.2	More Details

CVE Number	Description	Base Score	Reference
CVE-2023-41047	OctoPrint is a web interface for 3D printers. OctoPrint versions up until and including 1.9.2 contain a vulnerability that allows malicious admins to configure a specially crafted GCODE script that will allow code execution during rendering of that script. An attacker might use this to extract data managed by OctoPrint, or manipulate data managed by OctoPrint, as well as execute arbitrary commands with the rights of the OctoPrint process on the server system. OctoPrint versions from 1.9.3 onward have been patched. Administrators of OctoPrint instances are advised to make sure they can trust all other administrators on their instance and to also not blindly configure arbitrary GCODE scripts found online or provided to them by third parties.	6.2	More Details
CVE-2023-36126	There is a Cross Site Scripting (XSS) vulnerability in the "theme" parameter of preview.php in PHPJabbers Appointment Scheduler v3.0	6.1	More Details
CVE-2023-27121	A cross-site scripting (XSS) vulnerability in the component /framework/cron/action/humanize of Pleasant Solutions Pleasant Password Server v7.11.41.0 allows attackers to execute arbitrary web scripts or HTML via a crafted payload injected into the cronString parameter.	6.1	More Details
CVE-2023-36416	Microsoft Dynamics 365 (on-premises) Cross-site Scripting Vulnerability	6.1	More Details
CVE-2023-42808	Common Voice is the web app for Mozilla Common Voice, a platform for collecting speech donations in order to create public domain datasets for training voice recognition-related tools. Version 1.88.2 is vulnerable to reflected Cross-Site Scripting given that user-controlled data flows to a path expression (path of a network request). This issue may lead to reflected Cross-Site Scripting (XSS) in the context of Common Voice's server origin. As of time of publication, it is unknown whether any patches or workarounds exist.	6.1	More Details
CVE-2023-5375	Open Redirect in GitHub repository mosparo/mosparo prior to 1.0.2.	6.1	More Details
CVE-2023-4495	Easy Chat Server, in its 3.1 version and before, does not sufficiently encrypt user-controlled inputs, resulting in a Cross-Site Scripting (XSS) vulnerability stored via /registresult.htm (POST method), in the Resume parameter. The XSS is loaded from /register.ghp.	6.1	More Details

CVE Number	Description	Base Score	Reference
CVE-2023-4497	Easy Chat Server, in its 3.1 version and before, does not sufficiently encrypt user-controlled inputs, resulting in a Cross-Site Scripting (XSS) vulnerability stored via /registresult.htm (POST method), in the Icon parameter. The XSS is loaded from /users.ghp.	6.1	More Details
CVE-2023-5113	Certain HP Enterprise LaserJet and HP LaserJet Managed Printers are potentially vulnerable to denial of service due to WS-Print request and potential injections of Cross Site Scripting via jQuery-UI.	6.1	More Details
CVE-2023-45373	An issue was discovered in the ProofreadPage extension for MediaWiki before 1.35.12, 1.36.x through 1.39.x before 1.39.5, and 1.40.x before 1.40.1. XSS can occur via formatNumNoSeparators.	6.1	More Details
CVE-2023-43260	Milesight UR5X, UR32L, UR32, UR35, UR41 before v35.3.0.7 was discovered to contain a cross-site scripting (XSS) vulnerability via the admin panel.	6.1	More Details
CVE-2023-44390	HtmlSanitizer is a .NET library for cleaning HTML fragments and documents from constructs that can lead to XSS attacks. The vulnerability occurs in configurations where foreign content is allowed, i.e. either `svg` or `math` are in the list of allowed elements. In the case an application sanitizes user input with a vulnerable configuration, an attacker could bypass the sanitization and inject arbitrary HTML, including JavaScript code. Note that in the default configuration the vulnerability is not present. The vulnerability has been fixed in versions 8.0.723 and 8.1.722-beta (preview version).	6.1	More Details
CVE-2022-48183	A vulnerability was reported in ThinkPad T14s Gen 3 and X13 Gen3 that could cause the BIOS tamper detection mechanism to not trigger under specific circumstances which could allow unauthorized access.	6.1	More Details
CVE-2023-39193	A flaw was found in the Netfilter subsystem in the Linux kernel. The sctp_mt_check did not validate the flag_count field. This flaw allows a local privileged (CAP_NET_ADMIN) attacker to trigger an out-of-bounds read, leading to a crash or information disclosure.	6.1	More Details
CVE-2023-4496	Easy Chat Server, in its 3.1 version and before, does not sufficiently encrypt user-controlled inputs, resulting in a Cross-Site Scripting (XSS) vulnerability stored via /body2.ghp (POST method), in the mtowho parameter.	6.1	More Details

CVE Number	Description	Base Score	Reference
CVE-2023-4493	Stored Cross-Site Scripting in Easy Address Book Web Server 1.6 version, through the users_admin.ghp file that affects multiple parameters such as (firstname, homephone, lastname, lastname, middlename, workaddress, workcity, workcountry, workphone, workstate, workzip). This vulnerability allows a remote attacker to store a malicious JavaScript payload in the application to be executed when the page is loaded, resulting in an integrity impact.	6.1	More Details
CVE-2022-3728	A vulnerability was reported in ThinkPad T14s Gen 3 and X13 Gen3 that could cause the BIOS tamper detection mechanism to not trigger under specific circumstances which could allow unauthorized access.	6.1	More Details
CVE-2022-48182	A vulnerability was reported in ThinkPad T14s Gen 3 and X13 Gen3 that could cause the BIOS tamper detection mechanism to not trigger under specific circumstances which could allow unauthorized access.	6.1	More Details
CVE-2023-4492	Vulnerability in Easy Address Book Web Server 1.6 version, affecting the parameters (firstname, homephone, lastname, middlename, workaddress, workcity, workcountry, workphone, workstate and workzip) of the /addrbook.ghp file, allowing an attacker to inject a JavaScript payload specially designed to run when the application is loaded	6.1	More Details
CVE-2023-44812	Cross Site Scripting (XSS) vulnerability in mooSocial v.3.1.8 allows a remote attacker to execute arbitrary code via a crafted payload to the admin_redirect_url parameter of the user login function.	6.1	More Details
CVE-2023-43643	AntiSamy is a library for performing fast, configurable cleansing of HTML coming from untrusted sources. Prior to version 1.7.4, there is a potential for a mutation XSS (mXSS) vulnerability in AntiSamy caused by flawed parsing of the HTML being sanitized. To be subject to this vulnerability the `preserveComments` directive must be enabled in your policy file and also allow for certain tags at the same time. As a result, certain crafty inputs can result in elements in comment tags being interpreted as executable when using AntiSamy's sanitized output. This issue has been patched in AntiSamy 1.7.4 and later.	6.1	More Details
CVE-2023-44813	Cross Site Scripting (XSS) vulnerability in mooSocial v.3.1.8 allows a remote attacker to execute arbitrary code via a crafted payload to the mode parameter of the invite friend login function.	6.1	More Details
CVE-2022-4132	A flaw was found in JSS. A memory leak in JSS requires non-standard configuration but is a low-effort DoS vector if configured that way (repeatedly hitting the login page).	5.9	More Details

CVE Number	Description	Base Score	Reference
CVE-2023-42794	Incomplete Cleanup vulnerability in Apache Tomcat. The internal fork of Commons FileUpload packaged with Apache Tomcat 9.0.70 through 9.0.80 and 8.5.85 through 8.5.93 included an unreleased, in progress refactoring that exposed a potential denial of service on Windows if a web application opened a stream for an uploaded file but failed to close the stream. The file would never be deleted from disk creating the possibility of an eventual denial of service due to the disk being full. Users are recommended to upgrade to version 9.0.81 onwards or 8.5.94 onwards, which fixes the issue.	5.9	More Details
CVE-2023-5100	Cleartext Transmission of Sensitive Information in RDT400 in SICK APU allows an unprivileged remote attacker to retrieve potentially sensitive information via intercepting network traffic that is not encrypted.	5.9	More Details
CVE-2023-43804	urllib3 is a user-friendly HTTP client library for Python. urllib3 doesn't treat the `Cookie` HTTP header special or provide any helpers for managing cookies over HTTP, that is the responsibility of the user. However, it is possible for a user to specify a `Cookie` header and unknowingly leak information via HTTP redirects to a different origin if that user doesn't disable redirects explicitly. This issue has been patched in urllib3 version 1.26.17 or 2.0.5.	5.9	More Details
CVE-2023-30731	Logic error in package installation via debugger command prior to SMR Oct-2023 Release 1 allows physical attacker to install an application that has different build type.	5.7	More Details
CVE-2023-38537	A race condition in a network transport subsystem led to a heap use-after-free issue in established or unsilenced incoming audio/video calls that could have resulted in app termination or unexpected control flow with very low probability.	5.6	More Details
CVE-2023-41253	When on BIG-IP DNS or BIG-IP LTM enabled with DNS Services License, and a TSIG key is created, it is logged in plaintext in the audit log. Note: Software versions which have reached End of Technical Support (EoTS) are not evaluated.	5.5	More Details
CVE-2023-30732	Improper access control in system property prior to SMR Oct-2023 Release 1 allows local attacker to get CPU serial number.	5.5	More Details
CVE-2023-30738	An improper input validation in UEFI Firmware prior to Firmware update Oct-2023 Release in Galaxy Book, Galaxy Book Pro, Galaxy Book Pro 360 and Galaxy Book Odyssey allows local attacker to execute SMM memory corruption.	5.5	More Details

CVE Number	Description	Base Score	Reference
CVE-2023-3665	A code injection vulnerability in Trellix ENS 10.7.0 April 2023 release and earlier, allowed a local user to disable the ENS AMSI component via environment variables, leading to denial of service and or the execution of arbitrary code.	5.5	More Details
CVE-2023-43485	When TACACS+ audit forwarding is configured on BIG-IP or BIG-IQ system, sharedsecret is logged in plaintext in the audit log. Note: Software versions which have reached End of Technical Support (EoTS) are not evaluated.	5.5	More Details
CVE-2023-5370	On CPU 0 the check for the SMCCC workaround is called before SMCCC support has been initialized. This resulted in no speculative execution workarounds being installed on CPU 0.	5.5	More Details
CVE-2023-43786	A vulnerability was found in libX11 due to an infinite loop within the PutSubImage() function. This flaw allows a local user to consume all available system resources and cause a denial of service condition.	5.5	More Details
CVE-2023-43788	A vulnerability was found in libXpm due to a boundary condition within the XpmCreateXpmImageFromBuffer() function. This flaw allows a local attacker to trigger an out-of-bounds read error and read the contents of memory on the system.	5.5	More Details
CVE-2023-2422	A flaw was found in Keycloak. A Keycloak server configured to support mTLS authentication for OAuth/OpenID clients does not properly verify the client certificate chain. A client that possesses a proper certificate can authorize itself as any other client, therefore, access data that belongs to other clients.	5.5	More Details
CVE-2023-40645	In Messaging, there is a possible missing permission check. This could lead to local information disclosure with no additional execution privileges needed	5.5	More Details
CVE-2023-36713	Windows Common Log File System Driver Information Disclosure Vulnerability	5.5	More Details
CVE-2023-45245	Sensitive information disclosure due to missing authorization. The following products are affected: Acronis Agent (Linux, macOS, Windows) before build 36119.	5.5	More Details
CVE-2023-21291	In visitUris of Notification.java, there is a possible way to reveal image contents from another user due to a missing permission check. This could lead to local information disclosure with User execution privileges needed. User interaction is not needed for exploitation.	5.5	More Details

CVE Number	Description	Base Score	Reference
CVE-2023-5182	Sensitive data could be exposed in logs of subiquity version 23.09.1 and earlier. An attacker in the adm group could use this information to find hashed passwords and possibly escalate their privilege.	5.5	More Details
CVE-2023-36576	Windows Kernel Information Disclosure Vulnerability	5.5	More Details
CVE-2023-40633	In phasecheckserver, there is a possible missing permission check. This could lead to local information disclosure with no additional execution privileges needed	5.5	More Details
CVE-2023-40637	In telecom service, there is a possible missing permission check. This could lead to local information disclosure with no additional execution privileges	5.5	More Details
CVE-2023-40639	In SoundRecorder service, there is a possible missing permission check. This could lead to local information disclosure with no additional execution privileges	5.5	More Details
CVE-2023-40640	In SoundRecorder service, there is a possible missing permission check. This could lead to local information disclosure with no additional execution privileges	5.5	More Details
CVE-2023-40641	In Messaging, there is a possible missing permission check. This could lead to local information disclosure with no additional execution privileges needed	5.5	More Details
CVE-2023-40642	In Messaging, there is a possible missing permission check. This could lead to local information disclosure with no additional execution privileges needed	5.5	More Details
CVE-2023-40643	In Messaging, there is a possible missing permission check. This could lead to local information disclosure with no additional execution privileges needed	5.5	More Details
CVE-2023-40644	In Messaging, there is a possible missing permission check. This could lead to local information disclosure with no additional execution privileges needed	5.5	More Details
CVE-2023-40650	In Telecom service, there is a possible missing permission check. This could lead to local information disclosure with no additional execution privileges needed	5.5	More Details
CVE-2023-40649	In Messaging, there is a possible missing permission check. This could lead to local information disclosure with no additional execution privileges needed	5.5	More Details

CVE Number	Description	Base Score	Reference
CVE-2023-40648	In Messaging, there is a possible missing permission check. This could lead to local information disclosure with no additional execution privileges needed	5.5	More Details
CVE-2023-40647	In Messaging, there is a possible missing permission check. This could lead to local information disclosure with no additional execution privileges needed	5.5	More Details
CVE-2023-21253	In multiple locations, there is a possible way to crash multiple system services due to resource exhaustion. This could lead to local denial of service with no additional execution privileges needed. User interaction is not needed for exploitation.	5.5	More Details
CVE-2023-21252	In validatePassword of WifiConfigurationUtil.java, there is a possible way to get the device into a boot loop due to improper input validation. This could lead to local denial of service with no additional execution privileges needed. User interaction is not needed for exploitation.	5.5	More Details
CVE-2023-36724	Windows Power Management Service Information Disclosure Vulnerability	5.5	More Details
CVE-2023-42754	A NULL pointer dereference flaw was found in the Linux kernel ipv4 stack. The socket buffer (skb) was assumed to be associated with a device before calling __ip_options_compile, which is not always the case if the skb is re-routed by ipvs. This issue may allow a local user with CAP_NET_ADMIN privileges to crash the system.	5.5	More Details
CVE-2023-25604	An insertion of sensitive information into log file vulnerability in Fortinet FortiGuest 1.0.0 allows a local attacker to access plaintext passwords in the RADIUS logs.	5.5	More Details
CVE-2023-3576	A memory leak flaw was found in Libtiff's tiffcrop utility. This issue occurs when tiffcrop operates on a TIFF image file, allowing an attacker to pass a crafted TIFF image file to tiffcrop utility, which causes this memory leak issue, resulting an application crash, eventually leading to a denial of service.	5.5	More Details
CVE-2023-44210	Sensitive information disclosure and manipulation due to missing authorization. The following products are affected: Acronis Agent (Linux, macOS, Windows) before build 29258.	5.5	More Details
CVE-2023-26238	An issue was discovered in WatchGuard EPDR 8.0.21.0002. It is possible to enable or disable defensive capabilities by sending a crafted message to a named pipe.	5.5	More Details

CVE Number	Description	Base Score	Reference
CVE-2023-26239	An issue was discovered in WatchGuard EPDR 8.0.21.0002. Due to a weak implementation of a password check, it is possible to obtain credentials to access the management console as a non-privileged user.	5.5	More Details
CVE-2023-36728	Microsoft SQL Server Denial of Service Vulnerability	5.5	More Details
CVE-2023-40646	In Messaging, there is a possible missing permission check. This could lead to local information disclosure with no additional execution privileges needed	5.5	More Details
CVE-2023-44821	Gifsicle through 1.94, if deployed in a way that allows untrusted input to affect Gif_Realloc calls, might allow a denial of service (memory consumption). NOTE: this has been disputed by multiple parties because the Gifsicle code is not commonly used for unattended operation in which new input arrives for a long-running process, does not ship with functionality to link it into another application as a library, and does not have realistic use cases in which an adversary controls the entire command line.	5.5	More Details
CVE-2023-5441	NULL Pointer Dereference in GitHub repository vim/vim prior to 20d161ace307e28690229b68584f2d84556f8960.	5.5	More Details
CVE-2023-44213	Sensitive information disclosure due to excessive collection of system information. The following products are affected: Acronis Cyber Protect Cloud Agent (Windows) before build 35739, Acronis Cyber Protect 16 (Windows) before build 37391.	5.5	More Details
CVE-2023-44214	Sensitive information disclosure due to missing authorization. The following products are affected: Acronis Agent (Linux, macOS, Windows) before build 35739.	5.5	More Details
CVE-2023-45240	Sensitive information disclosure due to missing authorization. The following products are affected: Acronis Agent (Linux, macOS, Windows) before build 35739.	5.5	More Details
CVE-2023-45241	Sensitive information leak through log files. The following products are affected: Acronis Cyber Protect Cloud Agent (Linux, macOS, Windows) before build 35739, Acronis Cyber Protect 16 (Linux, macOS, Windows) before build 37391.	5.5	More Details
CVE-2023-45242	Sensitive information disclosure due to missing authorization. The following products are affected: Acronis Agent (Linux, macOS, Windows) before build 35739.	5.5	More Details

CVE Number	Description	Base Score	Reference
CVE-2023-45243	Sensitive information disclosure due to missing authorization. The following products are affected: Acronis Agent (Linux, macOS, Windows) before build 35739.	5.5	More Details
CVE-2023-44996	Cross-Site Request Forgery (CSRF) vulnerability in Naresh Parmar Post View Count plugin <= 1.8.2 versions.	5.4	More Details
CVE-2023-44470	Cross-Site Request Forgery (CSRF) vulnerability in Kvvaradha Kv TinyMCE Editor Add Fonts plugin <= 1.1 versions.	5.4	More Details
CVE-2023-44475	Cross-Site Request Forgery (CSRF) vulnerability in Michael Simpson Add Shortcodes Actions And Filters plugin <= 2.0.9 versions.	5.4	More Details
CVE-2023-36584	Windows Mark of the Web Security Feature Bypass Vulnerability	5.4	More Details
CVE-2023-44995	Cross-Site Request Forgery (CSRF) vulnerability in WP Doctor WooCommerce Login Redirect plugin <= 2.2.4 versions.	5.4	More Details
CVE-2023-26220	The Spotfire Library component of TIBCO Software Inc.'s Spotfire Analyst and Spotfire Server contains an easily exploitable vulnerability that allows a low privileged attacker with network access to execute a Stored Cross Site Scripting (XSS) on the affected system. A successful attack using this vulnerability requires human interaction from a person other than the attacker. Affected releases are TIBCO Software Inc.'s Spotfire Analyst: versions 11.4.7 and below, versions 11.5.0, 11.6.0, 11.7.0, 11.8.0, 12.0.0, 12.0.1, 12.0.2, 12.0.3, and 12.0.4, versions 12.1.0 and 12.1.1 and Spotfire Server: versions 11.4.11 and below, versions 11.5.0, 11.6.0, 11.6.1, 11.6.2, 11.6.3, 11.7.0, 11.8.0, 11.8.1, 12.0.0, 12.0.1, 12.0.2, 12.0.3, 12.0.4, and 12.0.5, versions 12.1.0 and 12.1.1.	5.4	More Details
CVE-2023-27433	Cross-Site Request Forgery (CSRF) vulnerability in YAS Global Team Make Paths Relative allows Cross Site Request Forgery.This issue affects Make Paths Relative: from n/a through 1.3.0.	5.4	More Details
CVE-2023-44762	A Cross Site Scripting (XSS) vulnerability in Concrete CMS from versions 9.2.0 to 9.2.2 allows an attacker to execute arbitrary code via a crafted script to the Tags from Settings - Tags.	5.4	More Details

CVE Number	Description	Base Score	Reference
CVE-2023-43343	Cross-site scripting (XSS) vulnerability in opensolution Quick CMS v.6.7 allows a local attacker to execute arbitrary code via a crafted script to the Files - Description parameter in the Pages Menu component.	5.4	More Details
CVE-2023-41670	Cross-Site Request Forgery (CSRF) vulnerability in Palasthotel (in person: Edward Bock) Use Memcached plugin <= 1.0.4 versions.	5.4	More Details
CVE-2023-41668	Cross-Site Request Forgery (CSRF) vulnerability in Leadster plugin <= 1.1.2 versions.	5.4	More Details
CVE-2023-30910	HPE MSA Controller prior to version IN210R004 could be remotely exploited to allow inconsistent interpretation of HTTP requests.	5.4	More Details
CVE-2023-44758	GDidees CMS 3.0 is affected by a Cross-Site Scripting (XSS) vulnerability that allows attackers to execute arbitrary code via a crafted payload to the Page Title.	5.4	More Details
CVE-2023-25033	Cross-Site Request Forgery (CSRF) vulnerability in Sumo Social Share Boost plugin <= 4.5 versions.	5.4	More Details
CVE-2023-44473	Cross-Site Request Forgery (CSRF) vulnerability in Michael Tran Table of Contents Plus plugin <= 2302 versions.	5.4	More Details
CVE-2023-27448	Cross-Site Request Forgery (CSRF) vulnerability in MakeStories Team MakeStories (for Google Web Stories) plugin <= 2.8.0 versions.	5.4	More Details
CVE-2023-27615	Cross-Site Request Forgery (CSRF) vulnerability in Dipak C. Gajjar WP Super Minify plugin <= 1.5.1 versions.	5.4	More Details
CVE-2023-44236	Cross-Site Request Forgery (CSRF) vulnerability in Devnath verma WP Captcha plugin <= 2.0.0 versions.	5.4	More Details
CVE-2023-44761	Multiple Cross Site Scripting (XSS) vulnerabilities in Concrete CMS versions affected to 8.5.13 and below, and 9.0.0 through 9.2.1 allow a local attacker to execute arbitrary code via a crafted script to the Forms of the Data objects.	5.4	More Details

CVE Number	Description	Base Score	Reference
CVE-2023-44764	A Cross Site Scripting (XSS) vulnerability in Concrete CMS before 9.2.3 exists via the Name parameter during installation (aka Site of Installation or Settings).	5.4	More Details
CVE-2023-44826	Cross Site Scripting vulnerability in ZenTaoPMS v.18.6 allows a local attacker to obtain sensitive information via a crafted script.	5.4	More Details
CVE-2023-44765	A Cross Site Scripting (XSS) vulnerability in Concrete CMS versions 8.5.12 and below, and 9.0 through 9.2.1 allows an attacker to execute arbitrary code via a crafted script to Plural Handle of the Data Objects from System & Settings.	5.4	More Details
CVE-2023-5452	Cross-site Scripting (XSS) - Stored in GitHub repository snipe/snipe-it prior to v6.2.2.	5.4	More Details
CVE-2023-44272	A cross-site scripting vulnerability exists in Citadel versions prior to 994. When a malicious user sends an instant message with some JavaScript code, the script may be executed on the web browser of the victim user.	5.4	More Details
CVE-2023-44770	A Cross-Site Scripting (XSS) vulnerability in Zenario CMS v.9.4.59197 allows an attacker to execute arbitrary code via a crafted script to the Organizer - Spare alias.	5.4	More Details
CVE-2023-44233	Cross-Site Request Forgery (CSRF) vulnerability in FooPlugins Best WordPress Gallery Plugin – FooGallery plugin <= 2.2.44 versions.	5.4	More Details
CVE-2023-44771	A Cross-Site Scripting (XSS) vulnerability in Zenario CMS v.9.4.59197 allows a local attacker to execute arbitrary code via a crafted script to the Page Layout.	5.4	More Details
CVE-2023-41950	Cross-Site Request Forgery (CSRF) vulnerability in Laposta - Roel Bousardt Laposta Signup Basic plugin <= 1.4.1 versions.	5.4	More Details
CVE-2023-41801	Cross-Site Request Forgery (CSRF) vulnerability in AWP Classifieds Team Ad Directory & Listings by AWP Classifieds plugin <= 4.3 versions.	5.4	More Details
CVE-2023-41732	Cross-Site Request Forgery (CSRF) vulnerability in CodePeople CP Blocks plugin <= 1.0.20 versions.	5.4	More Details

CVE Number	Description	Base Score	Reference
CVE-2023-41659	Cross-Site Request Forgery (CSRF) vulnerability in Jules Colle, BDWM Responsive Gallery Grid plugin <= 2.3.10 versions.	5.4	More Details
CVE-2023-41654	Cross-Site Request Forgery (CSRF) vulnerability in Andreas Heigl authLdap plugin <= 2.5.8 versions.	5.4	More Details
CVE-2023-42473	S/4HANA Manage (Withholding Tax Items) - version 106, does not perform necessary authorization checks for an authenticated user, resulting in escalation of privileges which has low impact on the confidentiality and integrity of the application.	5.4	More Details
CVE-2023-29235	Cross-Site Request Forgery (CSRF) vulnerability in Fugu Maintenance Switch plugin <= 1.5.2 versions.	5.4	More Details
CVE-2023-44075	Cross Site Scripting vulnerability in Small CRM in PHP v.3.0 allows a remote attacker to execute arbitrary code via a crafted payload to the Address parameter.	5.4	More Details
CVE-2023-41854	Cross-Site Request Forgery (CSRF) vulnerability in Softaculous Ltd. WpCentral plugin <= 1.5.7 versions.	5.4	More Details
CVE-2023-4090	Cross-site Scripting (XSS) reflected vulnerability on WideStand until 5.3.5 version, which generates one of the meta tags directly using the content of the queried URL, which would allow an attacker to inject HTML/Javascript code into the response.	5.4	More Details
CVE-2023-40561	Cross-Site Request Forgery (CSRF) vulnerability in theDotstore Enhanced Ecommerce Google Analytics for WooCommerce plugin <= 3.7.1 versions.	5.4	More Details
CVE-2023-44763	Concrete CMS v9.2.1 is affected by an Arbitrary File Upload vulnerability via a Thumbnail file upload, which allows Cross-Site Scripting (XSS). NOTE: the vendor's position is that a customer is supposed to know that "pdf" should be excluded from the allowed file types, even though pdf is one of the allowed file types in the default configuration.	5.4	More Details

CVE Number	Description	Base Score	Reference
CVE-2023-44399	ZITADEL provides identity infrastructure. In versions 2.37.2 and prior, ZITADEL administrators can enable a setting called "Ignoring unknown usernames" which helps mitigate attacks that try to guess/enumerate usernames. While this settings was properly working during the authentication process it did not work correctly on the password reset flow. This meant that even if this feature was active that an attacker could use the password reset function to verify if an account exist within ZITADEL. This bug has been patched in versions 2.37.3 and 2.38.0. No known workarounds are available.	5.3	More Details
CVE-2023-5371	RTPS dissector memory leak in Wireshark 4.0.0 to 4.0.8 and 3.6.0 to 3.6.16 allows denial of service via packet injection or crafted capture file	5.3	More Details
CVE-2021-3784	Garuda Linux performs an insecure user creation and authentication that allows any user to impersonate the created account. By creating users from the 'Garuda settings manager', an insecure procedure is performed that keeps the created user without an assigned password during some seconds. This could allow a potential attacker to exploit this vulnerability in order to authenticate without knowing the password.	5.3	More Details
CVE-2023-3153	A flaw was found in Open Virtual Network where the service monitor MAC does not properly rate limit. This issue could allow an attacker to cause a denial of service, including on deployments with CoPP enabled and properly configured.	5.3	More Details
CVE-2023-5101	Files or Directories Accessible to External Parties in RDT400 in SICK APU allows an unprivileged remote attacker to download various files from the server via HTTP requests.	5.3	More Details
CVE-2023-5102	Insufficient Control Flow Management in RDT400 in SICK APU allows an unprivileged remote attacker to potentially enable hidden functionality via HTTP requests.	5.3	More Details
CVE-2023-4469	The Profile Extra Fields by BestWebSoft plugin for WordPress is vulnerable to unauthorized access of data due to a missing capability check on the prflxtrflds_export_file function in versions up to, and including, 1.2.7. This makes it possible for unauthenticated attackers to expose potentially sensitive user data, including data entered into custom fields.	5.3	More Details
CVE-2023-45374	An issue was discovered in the SportsTeams extension for MediaWiki before 1.35.12, 1.36.x through 1.39.x before 1.39.5, and 1.40.x before 1.40.1. It does not check for the anti-CSRF edit token in Special:SportsTeamsManager and Special:UpdateFavoriteTeams.	5.3	More Details

CVE Number	Description	Base Score	Reference
CVE-2023-45372	An issue was discovered in the Wikibase extension for MediaWiki before 1.35.12, 1.36.x through 1.39.x before 1.39.5, and 1.40.x before 1.40.1. During item merging, ItemMergeInteractor does not have an edit filter running (e.g., AbuseFilter).	5.3	More Details
CVE-2023-43058	IBM Robotic Process Automation 23.0.9 is vulnerable to privilege escalation that affects ownership of projects. IBM X-Force ID: 247527.	5.3	More Details
CVE-2023-45370	An issue was discovered in the SportsTeams extension for MediaWiki before 1.35.12, 1.36.x through 1.39.x before 1.39.5, and 1.40.x before 1.40.1. SportsTeams: Special:SportsManagerLogo and Special:SportsTeamsManagerLogo do not check for the sportsteamsmanager user right, and thus an attacker may be able to affect pages that are concerned with sports teams.	5.3	More Details
CVE-2023-45364	An issue was discovered in includes/page/Article.php in MediaWiki 1.36.x through 1.39.x before 1.39.5 and 1.40.x before 1.40.1. Deleted revision existence is leaked due to incorrect permissions being checked. This reveals that a given revision ID belonged to the given page title, and its timestamp, both of which are not supposed to be public information.	5.3	More Details
CVE-2023-44386	Vapor is an HTTP web framework for Swift. There is a denial of service vulnerability impacting all users of affected versions of Vapor. The HTTP1 error handler closed connections when HTTP parse errors occur instead of passing them on. The issue is fixed as of Vapor release 4.84.2.	5.3	More Details
CVE-2023-42795	Incomplete Cleanup vulnerability in Apache Tomcat.When recycling various internal objects in Apache Tomcat from 11.0.0-M1 through 11.0.0-M11, from 10.1.0-M1 through 10.1.13, from 9.0.0-M1 through 9.0.80 and from 8.5.0 through 8.5.93, an error could cause Tomcat to skip some parts of the recycling process leading to information leaking from the current request/response to the next. Users are recommended to upgrade to version 11.0.0-M12 onwards, 10.1.14 onwards, 9.0.81 onwards or 8.5.94 onwards, which fixes the issue.	5.3	More Details
CVE-2023-43623	A vulnerability has been identified in Mendix Forgot Password (Mendix 10 compatible) (All versions < V5.4.0), Mendix Forgot Password (Mendix 7 compatible) (All versions < V3.7.3), Mendix Forgot Password (Mendix 8 compatible) (All versions < V4.1.3), Mendix Forgot Password (Mendix 9 compatible) (All versions < V5.4.0). Applications using the affected module are vulnerable to user enumeration due to distinguishable responses. This could allow an unauthenticated remote attacker to determine if a user is valid or not, enabling a brute force attack with valid users.	5.3	More Details

CVE Number	Description	Base Score	Reference
CVE-2023-42782	A insufficient verification of data authenticity vulnerability [CWE-345] in FortiAnalyzer version 7.4.0 and below 7.2.3 allows a remote unauthenticated attacker to send messages to the syslog server of FortiAnalyzer via the knoweldge of an authorized device serial number.	5.3	More Details
CVE-2023-41763	Skype for Business Elevation of Privilege Vulnerability	5.3	More Details
CVE-2023-41675	A use after free vulnerability [CWE-416] in FortiOS version 7.2.0 through 7.2.4 and version 7.0.0 through 7.0.10 and FortiProxy version 7.2.0 through 7.2.2 and version 7.0.0 through 7.0.8 may allow an unauthenticated remote attacker to crash the WAD process via multiple crafted packets reaching proxy policies or firewall policies with proxy mode alongside SSL deep packet inspection.	5.3	More Details
CVE-2023-45648	Improper Input Validation vulnerability in Apache Tomcat.Tomcat from 11.0.0-M1 through 11.0.0-M11, from 10.1.0-M1 through 10.1.13, from 9.0.0-M1 through 9.0.81 and from 8.5.0 through 8.5.93 did not correctly parse HTTP trailer headers. A specially crafted, invalid trailer header could cause Tomcat to treat a single request as multiple requests leading to the possibility of request smuggling when behind a reverse proxy. Users are recommended to upgrade to version 11.0.0-M12 onwards, 10.1.14 onwards, 9.0.81 onwards or 8.5.94 onwards, which fix the issue.	5.3	More Details
CVE-2023-30802	The Sangfor Next-Gen Application Firewall version NGAF8.0.17 is vulnerable to a source code disclosure vulnerability. A remote and unauthenticated attacker can obtain PHP source code by sending an HTTP request with an invalid Content-Length field.	5.3	More Details
CVE-2023-3213	The WP Mail SMTP Pro plugin for WordPress is vulnerable to unauthorized access of data due to a missing capability check on the is_print_page function in versions up to, and including, 3.8.0. This makes it possible for unauthenticated attackers to disclose potentially sensitive email information.	5.3	More Details
CVE-2023-40376	IBM UrbanCode Deploy (UCD) 7.1 - 7.1.2.12, 7.2 through 7.2.3.5, and 7.3 through 7.3.2.0 under certain configurations could allow an authenticated user to make changes to environment variables due to improper authentication controls. IBM X-Force ID: 263581.	5.3	More Details
CVE-2023-23371	A cleartext transmission of sensitive information vulnerability has been reported to affect QVPN Device Client. If exploited, the vulnerability could allow local authenticated administrators to read sensitive data via unspecified vectors. We have already fixed the vulnerability in the following version: QVPN Windows 2.2.0.0823 and later	5.2	More Details

CVE Number	Description	Base Score	Reference
CVE-2023-39189	A flaw was found in the Netfilter subsystem in the Linux kernel. The nfnl_osf_add_callback function did not validate the user mode controlled opt_num field. This flaw allows a local privileged (CAP_NET_ADMIN) attacker to trigger an out-of-bounds read, leading to a crash or information disclosure.	5.1	More Details
CVE-2023-30735	Improper Preservation of Permissions vulnerability in SAssistant prior to version 8.7 allows local attackers to access backup data in SAssistant.	5.1	More Details
CVE-2023-43799	Altair is a GraphQL Client. Prior to version 5.2.5, the Altair GraphQL Client Desktop Application does not sanitize external URLs before passing them to the underlying system. Moreover, Altair GraphQL Client also does not isolate the context of the renderer process. This affects versions of the software running on MacOS, Windows, and Linux. Version 5.2.5 fixes this issue.	5.0	More Details
CVE-2023-38538	A race condition in an event subsystem led to a heap use-after-free issue in established audio/video calls that could have resulted in app termination or unexpected control flow with very low probability.	5.0	More Details
CVE-2023-30804	The Sangfor Next-Gen Application Firewall version NGAF8.0.17 is vulnerable to an authenticated file disclosure vulnerability. A remote and authenticated attacker can read arbitrary system files using the svpn_html/loadfile.php endpoint. This issue is exploitable by a remote and unauthenticated attacker when paired with CVE-2023-30803.	4.9	More Details
CVE-2023-45129	Synapse is an open-source Matrix homeserver written and maintained by the Matrix.org Foundation. Prior to version 1.94.0, a malicious server ACL event can impact performance temporarily or permanently leading to a persistent denial of service. Homeservers running on a closed federation (which presumably do not need to use server ACLs) are not affected. Server administrators are advised to upgrade to Synapse 1.94.0 or later. As a workaround, rooms with malicious server ACL events can be purged and blocked using the admin API.	4.9	More Details
CVE-2023-36820	Micronaut Security is a security solution for applications. Prior to versions 3.1.2, 3.2.4, 3.3.2, 3.4.3, 3.5.3, 3.6.6, 3.7.4, 3.8.4, 3.9.6, 3.10.2, and 3.11.1, IdTokenClaimsValidator skips `aud` claim validation if token is issued by same identity issuer/provider. Any OIDC setup using Micronaut where multiple OIDC applications exists for the same issuer but token auth are not meant to be shared. This issue has been patched in versions 3.1.2, 3.2.4, 3.3.2, 3.4.3, 3.5.3, 3.6.6, 3.7.4, 3.8.4, 3.9.6, 3.10.2, and 3.11.1.	4.8	More Details

CVE Number	Description	Base Score	Reference
CVE-2023-43877	Rite CMS 3.0 has Multiple Cross-Site scripting (XSS) vulnerabilities that allow attackers to execute arbitrary code via a payload crafted in the Home Page fields in the Administration menu.	4.8	More Details
CVE-2023-44766	A Cross Site Scripting (XSS) vulnerability in Concrete CMS v.9.2.1 allows an attacker to execute arbitrary code via a crafted script to the SEO - Extra from Page Settings. NOTE: the vendor disputes this because this SEO-related header change can only be made by an admin, and allowing an admin to place JavaScript there is an intentional customization feature.	4.8	More Details
CVE-2023-44315	A vulnerability has been identified in SINEC NMS (All versions < V2.0). The affected application improperly sanitizes certain SNMP configuration data retrieved from monitored devices. An attacker with access to a monitored device could prepare a stored cross-site scripting (XSS) attack that may lead to unintentional modification of application data by legitimate users.	4.7	More Details
CVE-2023-5423	A vulnerability has been found in SourceCodester Online Pizza Ordering System 1.0 and classified as critical. This vulnerability affects unknown code of the file /admin/ajax.php?action=confirm_order. The manipulation of the argument id leads to sql injection. The attack can be initiated remotely. The identifier of this vulnerability is VDB-241384.	4.7	More Details
CVE-2023-40684	IBM Content Navigator 3.0.11, 3.0.13, and 3.0.14 with IBM Daeja ViewOne Virtual is vulnerable to cross-site scripting. This vulnerability allows users to embed arbitrary JavaScript code in the Web UI thus altering the intended functionality potentially leading to credentials disclosure within a trusted session. IBM X-Force ID: 264019.	4.6	More Details
CVE-2023-35905	IBM FileNet Content Manager 5.5.8, 5.5.10, and 5.5.11 is vulnerable to cross-site scripting. This vulnerability allows users to embed arbitrary JavaScript code in the Web UI thus altering the intended functionality potentially leading to credentials disclosure within a trusted session. IBM X-Force ID: 259384.	4.6	More Details
CVE-2023-40651	In urild service, there is a possible out of bounds write due to a missing bounds check. This could lead to local denial of service with System execution privileges needed	4.4	More Details
CVE-2023-40636	In telecom service, there is a possible way to write permission usage records of an app due to a missing permission check. This could lead to local information disclosure with System execution privileges needed	4.4	More Details

CVE Number	Description	Base Score	Reference
CVE-2023-43071	Dell SmartFabric Storage Software v1.4 (and earlier) contains possible vulnerabilities for HTML injection or CVS formula injection which might escalate to cross-site scripting attacks in HTML pages in the GUI. A remote authenticated attacker could potentially exploit these issues, leading to various injection type attacks.	4.4	More Details
CVE-2023-30736	Improper authorization in PushMsgReceiver of Samsung Assistant prior to version 8.7.00.1 allows attacker to execute javascript interface. To trigger this vulnerability, user interaction is required.	4.4	More Details
CVE-2023-45219	Exposure of Sensitive Information vulnerability exist in an undisclosed BIG-IP TMOS shell (tmsh) command which may allow an authenticated attacker with resource administrator role privileges to view sensitive information. Note: Software versions which have reached End of Technical Support (EoTS) are not evaluated.	4.4	More Details
CVE-2023-40631	In Dialer, there is a possible missing permission check. This could lead to local information disclosure with System execution privileges needed	4.4	More Details
CVE-2023-36698	Windows Kernel Security Feature Bypass Vulnerability	4.4	More Details
CVE-2023-40638	In Telecom service, there is a possible missing permission check. This could lead to local denial of service with System execution privileges needed	4.4	More Details
CVE-2022-3248	A flaw was found in OpenShift API, as admission checks do not enforce "custom-host" permissions. This issue could allow an attacker to violate the boundaries, as permissions will not be applied.	4.4	More Details
CVE-2023-40652	In jpg driver, there is a possible out of bounds write due to improper input validation. This could lead to local denial of service with System execution privileges needed	4.4	More Details
CVE-2023-37195	A vulnerability has been identified in SIMATIC CP 1604 (All versions), SIMATIC CP 1616 (All versions), SIMATIC CP 1623 (All versions), SIMATIC CP 1626 (All versions), SIMATIC CP 1628 (All versions). Affected devices insufficiently control continuous mapping of direct memory access (DMA) requests. This could allow local attackers with administrative privileges to cause a denial of service situation on the host. A physical power cycle is required to get the system working again.	4.4	More Details

CVE Number	Description	Base Score	Reference
CVE-2023-36722	Active Directory Domain Services Information Disclosure Vulnerability	4.4	More Details
CVE-2023-39447	When BIG-IP APM Guided Configurations are configured, undisclosed sensitive information may be logged in restnoded log. Note: Software versions which have reached End of Technical Support (EoTS) are not evaluated.	4.4	More Details
CVE-2023-43072	Dell SmartFabric Storage Software v1.4 (and earlier) contains an improper access control vulnerability in the CLI. A local possibly unauthenticated attacker could potentially exploit this vulnerability, leading to ability to execute arbitrary shell commands.	4.4	More Details
CVE-2023-37995	Cross-Site Request Forgery (CSRF) vulnerability in Chetan Gole WP-CopyProtect [Protect your blog posts] plugin <= 3.1.0 versions.	4.3	More Details
CVE-2023-28791	Cross-Site Request Forgery (CSRF) vulnerability in Gangesh Matta Simple Org Chart plugin <= 2.3.4 versions.	4.3	More Details
CVE-2023-40008	Cross-Site Request Forgery (CSRF) vulnerability in Gangesh Matta Simple Org Chart plugin <= 2.3.4 versions.	4.3	More Details
CVE-2023-40556	Cross-Site Request Forgery (CSRF) vulnerability in Greg Ross Schedule Posts Calendar plugin <= 5.2 versions.	4.3	More Details
CVE-2015-10125	A vulnerability classified as problematic has been found in WP Ultimate CSV Importer Plugin 3.7.2 on WordPress. This affects an unknown part. The manipulation leads to cross-site request forgery. It is possible to initiate the attack remotely. Upgrading to version 3.7.3 is able to address this issue. The identifier of the patch is 13c30af721d3f989caac72dd0f56cf0dc40fad7e. It is recommended to upgrade the affected component. The identifier VDB-241317 was assigned to this vulnerability.	4.3	More Details
CVE-2022-4145	A content spoofing flaw was found in OpenShift's OAuth endpoint. This flaw allows a remote, unauthenticated attacker to inject text into a webpage, enabling the obfuscation of a phishing operation.	4.3	More Details
CVE-2023-40671	Cross-Site Request Forgery (CSRF) vulnerability in 大侠wp DX-auto-save-images plugin <= 1.4.0 versions.	4.3	More Details

CVE Number	Description	Base Score	Reference
CVE-2023-25980	Cross-Site Request Forgery (CSRF) vulnerability in CAGE Web Design | Rolf van Gelder Optimize Database after Deleting Revisions plugin <= 5.1 versions.	4.3	More Details
CVE-2023-40559	Cross-Site Request Forgery (CSRF) vulnerability in theDotstore Dynamic Pricing and Discount Rules for WooCommerce plugin <= 2.4.0 versions.	4.3	More Details
CVE-2022-47175	Cross-Site Request Forgery (CSRF) vulnerability in P Royal Royal Elementor Addons and Templates plugin <= 1.3.75 versions.	4.3	More Details
CVE-2023-25480	Cross-Site Request Forgery (CSRF) vulnerability in BoldGrid Post and Page Builder by BoldGrid – Visual Drag and Drop Editor plugin <= 1.24.1 versions.	4.3	More Details
CVE-2023-43073	Dell SmartFabric Storage Software v1.4 (and earlier) contains an Improper Input Validation vulnerability in RADIUS configuration. An authenticated remote attacker could potentially exploit this vulnerability, leading to gaining unauthorized access to data.	4.3	More Details
CVE-2023-44241	Cross-Site Request Forgery (CSRF) vulnerability in Keap Keap Landing Pages plugin <= 1.4.2 versions.	4.3	More Details
CVE-2023-40607	Cross-Site Request Forgery (CSRF) vulnerability in CLUEVO CLUEVO LMS, E-Learning Platform plugin <= 1.10.0 versions.	4.3	More Details
CVE-2023-41650	Cross-Site Request Forgery (CSRF) vulnerability in Venugopal Remove/hide Author, Date, Category Like Entry-Meta plugin <= 2.1 versions.	4.3	More Details
CVE-2023-42475	The Statutory Reporting application has a vulnerable file storage location, potentially enabling low privileged attacker to read server files with minimal impact on confidentiality.	4.3	More Details
CVE-2023-41684	Cross-Site Request Forgery (CSRF) vulnerability in Felix Welberg SIS Handball plugin <= 1.0.45 versions.	4.3	More Details
CVE-2023-41694	Cross-Site Request Forgery (CSRF) vulnerability in Realbig Team Realbig For WordPress plugin <= 1.0.3 versions.	4.3	More Details

CVE Number	Description	Base Score	Reference
CVE-2023-41697	Cross-Site Request Forgery (CSRF) vulnerability in Nikunj Soni Easy WP Cleaner plugin <= 1.9 versions.	4.3	More Details
CVE-2023-41730	Cross-Site Request Forgery (CSRF) vulnerability in SendPress Newsletters plugin <= 1.22.3.31 versions.	4.3	More Details
CVE-2023-41850	Cross-Site Request Forgery (CSRF) vulnerability in Morris Bryant, Ruben Sargsyan Outbound Link Manager plugin <= 1.2 versions.	4.3	More Details
CVE-2023-41851	Cross-Site Request Forgery (CSRF) vulnerability in Dotsquares WP Custom Post Template <= 1.0 versions.	4.3	More Details
CVE-2023-41852	Cross-Site Request Forgery (CSRF) vulnerability in MailMunch MailMunch – Grow your Email List plugin <= 3.1.2 versions.	4.3	More Details
CVE-2023-41853	Cross-Site Request Forgery (CSRF) vulnerability in WP iCal Availability plugin <= 1.0.3 versions.	4.3	More Details
CVE-2023-41858	Cross-Site Request Forgery (CSRF) vulnerability in Ashok Rane Order Delivery Date for WP e-Commerce plugin <= 1.2 versions.	4.3	More Details
CVE-2023-41876	Cross-Site Request Forgery (CSRF) vulnerability in Hardik Kalathiya WP Gallery Metabox plugin <= 1.0.0 versions.	4.3	More Details
CVE-2023-44257	Cross-Site Request Forgery (CSRF) vulnerability in Hometory Mang Board WP plugin <= 1.7.6 versions.	4.3	More Details
CVE-2023-44259	Cross-Site Request Forgery (CSRF) vulnerability in Mediavine Mediavine Control Panel plugin <= 2.10.2 versions.	4.3	More Details
CVE-2023-44261	Cross-Site Request Forgery (CSRF) vulnerability in Dinesh Karki Block Plugin Update plugin <= 3.3 versions.	4.3	More Details
CVE-2023-5498	Cross-Site Request Forgery (CSRF) in GitHub repository chiefonboarding/chiefonboarding prior to v2.0.47.	4.3	More Details

CVE Number	Description	Base Score	Reference
CVE-2023-44994	Cross-Site Request Forgery (CSRF) vulnerability in Bainternet ShortCodes UI plugin <= 1.9.8 versions.	4.3	More Details
CVE-2023-44476	Cross-Site Request Forgery (CSRF) vulnerability in Andres Felipe Perea V. CopyRightPro plugin <= 2.1 versions.	4.3	More Details
CVE-2023-44471	Cross-Site Request Forgery (CSRF) vulnerability in Bernhard Kau Backend Localization plugin <= 2.1.10 versions.	4.3	More Details
CVE-2023-41964	The BIG-IP and BIG-IQ systems do not encrypt some sensitive information written to Database (DB) variables. Note: Software versions which have reached End of Technical Support (EoTS) are not evaluated.	4.3	More Details
CVE-2023-41365	SAP Business One (B1i) - version 10.0, allows an authorized attacker to retrieve the details stack trace of the fault message to conduct the XXE injection, which will lead to information disclosure. After successful exploitation, an attacker can cause limited impact on the confidentiality and no impact to the integrity and availability.	4.3	More Details
CVE-2023-41672	Cross-Site Request Forgery (CSRF) vulnerability in Rémi Leclercq Hide admin notices – Admin Notification Center plugin <= 2.3.2 versions.	4.3	More Details
CVE-2023-41669	Cross-Site Request Forgery (CSRF) vulnerability in DAEXT Live News plugin <= 1.06 versions.	4.3	More Details
CVE-2023-44238	Cross-Site Request Forgery (CSRF) vulnerability in Joakim Ling Remove slug from custom post type plugin <= 1.0.3 versions.	4.3	More Details
CVE-2023-44146	Cross-Site Request Forgery (CSRF) vulnerability in Checkfront Inc. Checkfront Online Booking System plugin <= 3.6 versions.	4.3	More Details
CVE-2023-44243	Cross-Site Request Forgery (CSRF) vulnerability in Dylan Blokhuis Instant CSS plugin <= 1.2.1 versions.	4.3	More Details
CVE-2023-25489	Cross-Site Request Forgery (CSRF) vulnerability in Jeff Sherk Update Theme and Plugins from Zip File plugin <= 2.0.0 versions.	4.3	More Details

CVE Number	Description	Base Score	Reference
CVE-2023-25025	Cross-Site Request Forgery (CSRF) vulnerability in Chetan Gole WP-CopyProtect [Protect your blog posts] plugin <= 3.1.0 versions.	4.3	More Details
CVE-2023-44231	Cross-Site Request Forgery (CSRF) vulnerability in NickDuncan Contact Form plugin <= 2.0.10 versions.	4.3	More Details
CVE-2023-44232	Cross-Site Request Forgery (CSRF) vulnerability in Huseyin Berberoglu WP Hide Pages plugin <= 1.0 versions.	4.3	More Details
CVE-2023-44260	Cross-Site Request Forgery (CSRF) vulnerability in Mikk Mihkel Nurges, Rebing OÜ Woocommerce ESTO plugin <= 2.23.1 versions.	4.3	More Details
CVE-2023-44237	Cross-Site Request Forgery (CSRF) vulnerability in Moriyan Jay WP Site Protector plugin <= 2.0 versions.	4.3	More Details
CVE-2023-44246	Cross-Site Request Forgery (CSRF) vulnerability in Matias s Shockingly Simple Favicon plugin <= 1.8.2 versions.	4.3	More Details
CVE-2023-44240	Cross-Site Request Forgery (CSRF) vulnerability in Peter Butler Timthumb Vulnerability Scanner plugin <= 1.54 versions.	4.3	More Details
CVE-2023-44993	Cross-Site Request Forgery (CSRF) vulnerability in QuantumCloud AI ChatBot plugin <= 4.7.8 versions.	4.3	More Details
CVE-2023-5330	Mattermost fails to enforce a limit for the size of the cache entry for OpenGraph data allowing an attacker to send a specially crafted request to the /api/v4/opengraph filling the cache and turning the server unavailable.	4.3	More Details
CVE-2023-5331	Mattermost fails to properly check the creator of an attached file when adding the file to a draft post, potentially exposing unauthorized file information.	4.3	More Details
CVE-2023-5333	Mattermost fails to deduplicate input IDs allowing a simple user to cause the application to consume excessive resources and possibly crash by sending a specially crafted request to /api/v4/users/ids with multiple identical IDs.	4.3	More Details

CVE Number	Description	Base Score	Reference
CVE-2023-5103	Improper Restriction of Rendered UI Layers or Frames in RDT400 in SICK APU allows an unprivileged remote attacker to potentially reveal sensitive information via tricking a user into clicking on an actionable item using an iframe.	4.3	More Details
CVE-2023-44249	An authorization bypass through user-controlled key [CWE-639] vulnerability in Fortinet FortiManager version 7.4.0 and before 7.2.3 and FortiAnalyzer version 7.4.0 and before 7.2.3 allows a remote attacker with low privileges to read sensitive information via crafted HTTP requests.	4.3	More Details
CVE-2023-41667	Cross-Site Request Forgery (CSRF) vulnerability in Ulf Benjaminsson WP-dTree plugin <= 4.4.5 versions.	4.3	More Details
CVE-2023-45369	An issue was discovered in the PageTriage extension for MediaWiki before 1.35.12, 1.36.x through 1.39.x before 1.39.5, and 1.40.x before 1.40.1. Usernames of hidden users are exposed.	4.3	More Details
CVE-2023-44384	Discourse-jira is a Discourse plugin allows Jira projects, issue types, fields and field options will be synced automatically. An administrator user can make an SSRF attack by setting the Jira URL to an arbitrary location and enabling the `discourse_jira_verbose_log` site setting. A moderator user could manipulate the request path to the Jira API, allowing them to perform arbitrary GET requests using the Jira API credentials, potentially with elevated permissions, used by the application.	4.1	More Details
CVE-2023-30734	Improper access control vulnerability in Samsung Health prior to version 6.24.3.007 allows attackers to access sensitive information via implicit intent.	4.0	More Details
CVE-2023-30737	Improper access control vulnerability in Samsung Health prior to version 6.24.3.007 allows attackers to access sensitive information via implicit intent.	4.0	More Details
CVE-2022-34355	IBM Jazz Foundation (IBM Engineering Lifecycle Management 6.0.6, 6.0.6.1, 7.0, 7.0.1, and 7.0.2) could disclose sensitive version information to a user that could be used in further attacks against the system. IBM X-Force ID: 230498.	4.0	More Details
CVE-2022-22447	IBM Disconnected Log Collector 1.0 through 1.8.2 is vulnerable to potential security misconfigurations that could disclose unintended information. IBM X-Force ID: 224648.	4.0	More Details

CVE Number	Description	Base Score	Reference
CVE-2023-36555	An improper neutralization of script-related html tags in a web page (basic xss) in Fortinet FortiOS 7.2.0 - 7.2.4 allows an attacker to execute unauthorized code or commands via the SAML and Security Fabric components.	3.9	More Details
CVE-2023-32971	A buffer copy without checking size of input vulnerability has been reported to affect several QNAP operating system versions. If exploited, the vulnerability could allow authenticated administrators to execute code via a network. We have already fixed the vulnerability in the following versions: QTS 5.0.1.2425 build 20230609 and later QTS 5.1.0.2444 build 20230629 and later QTS 4.5.4.2467 build 20230718 and later QuTS hero h5.0.1.2515 build 20230907 and later QuTS hero h5.1.0.2424 build 20230609 and later QuTS hero h4.5.4.2476 build 20230728 and later QuTScloud c5.1.0.2498 and later	3.8	More Details
CVE-2023-32972	A buffer copy without checking size of input vulnerability has been reported to affect several QNAP operating system versions. If exploited, the vulnerability could allow authenticated administrators to execute code via a network. We have already fixed the vulnerability in the following versions: QTS 5.0.1.2425 build 20230609 and later QTS 5.1.0.2444 build 20230629 and later QTS 4.5.4.2467 build 20230718 and later QuTS hero h5.0.1.2515 build 20230907 and later QuTS hero h5.1.0.2424 build 20230609 and later QuTS hero h4.5.4.2476 build 20230728 and later QuTScloud c5.1.0.2498 and later	3.8	More Details
CVE-2022-33160	IBM Security Directory Suite 8.0.1 uses weaker than expected cryptographic algorithms that could allow an attacker to decrypt highly sensitive information. IBM X-Force ID: 228568.	3.7	More Details
CVE-2023-5461	A vulnerability was found in Delta Electronics WPLSoft 2.51. It has been classified as problematic. Affected is an unknown function of the component Modbus Handler. The manipulation leads to cleartext transmission of sensitive information. It is possible to launch the attack remotely. The complexity of an attack is rather high. The exploitability is told to be difficult. The exploit has been disclosed to the public and may be used. The identifier of this vulnerability is VDB-241584. NOTE: The vendor was contacted early about this disclosure but did not respond in any way.	3.7	More Details

CVE Number	Description	Base Score	Reference
CVE-2023-5460	A vulnerability was found in Delta Electronics WPLSoft up to 2.51 and classified as problematic. This issue affects some unknown processing of the component Modbus Data Packet Handler. The manipulation leads to heap-based buffer overflow. The exploit has been disclosed to the public and may be used. The associated identifier of this vulnerability is VDB-241583. NOTE: The vendor was contacted early about this disclosure but did not respond in any way.	3.5	More Details
CVE-2023-36637	An improper neutralization of input during web page generation vulnerability [CWE-79] in FortiMail version 7.2.0 through 7.2.2 and before 7.0.5 allows an authenticated attacker to inject HTML tags in FortiMail's calendar via input fields.	3.5	More Details
CVE-2023-37939	An exposure of sensitive information to an unauthorized actor vulnerability [CWE-200] in FortiClient for Windows 7.2.0, 7.0 all versions, 6.4 all versions, 6.2 all versions, Linux 7.2.0, 7.0 all versions, 6.4 all versions, 6.2 all versions and Mac 7.2.0 through 7.2.1, 7.0 all versions, 6.4 all versions, 6.2 all versions, may allow a local authenticated attacker with no Administrative privileges to retrieve the list of files or folders excluded from malware scanning.	3.3	More Details
CVE-2023-44387	Gradle is a build tool with a focus on build automation and support for multi-language development. When copying or archiving symlinked files, Gradle resolves them but applies the permissions of the symlink itself instead of the permissions of the linked file to the resulting file. This leads to files having too much permissions given that symlinks usually are world readable and writeable. While it is unlikely this results in a direct vulnerability for the impacted build, it may open up attack vectors depending on where build artifacts end up being copied to or un-archived. In versions 7.6.3, 8.4 and above, Gradle will now properly use the permissions of the file pointed at by the symlink to set permissions of the copied or archived file.	3.2	More Details
CVE-2023-39194	A flaw was found in the XFRM subsystem in the Linux kernel. The specific flaw exists within the processing of state filters, which can result in a read past the end of an allocated buffer. This flaw allows a local privileged (CAP_NET_ADMIN) attacker to trigger an out-of-bounds read, potentially leading to an information disclosure.	3.2	More Details
CVE-2022-43906	IBM Security Guardium 11.5 could disclose sensitive information due to a missing or insecure SameSite attribute for a sensitive cookie. IBM X-Force ID: 240897.	3.1	More Details

CVE Number	Description	Base Score	Reference
CVE-2023-44389	Zope is an open-source web application server. The title property, available on most Zope objects, can be used to store script code that is executed while viewing the affected object in the Zope Management Interface (ZMI). All versions of Zope 4 and Zope 5 are affected. Patches will be released with Zope versions 4.8.11 and 5.8.6.	3.1	More Details
CVE-2023-5496	A vulnerability was found in Translator PoqDev Add-On 1.0.11 on Firefox. It has been rated as problematic. This issue affects some unknown processing of the component Select Text Handler. The manipulation leads to cross site scripting. The attack may be initiated remotely. The complexity of an attack is rather high. The exploitation is known to be difficult. The exploit has been disclosed to the public and may be used. The identifier VDB-241649 was assigned to this vulnerability. NOTE: The vendor was contacted early about this disclosure but did not respond in any way.	3.1	More Details
CVE-2023-4567	Rejected reason: Issue has been found to be non-reproducible, therefore not a viable flaw.	N/A	More Details
CVE-2023-5312	Rejected reason: ** REJECT ** DO NOT USE THIS CANDIDATE NUMBER. ConsultIDs: CVE-2023-43226. Reason: This candidate is a reservation duplicate of CVE-2023-43226. Notes: All CVE users should reference CVE-2023-43226 instead of this candidate. All references and descriptions in this candidate have been removed to prevent accidental usage.	N/A	More Details