SingCERT
Singapore Cyber Emergency Response Team

Security Bulletin 14 September 2022

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

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

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

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

CRITICAL VULNERABILITIES

CVE Number	Description	Base Score	Reference
CVE-2022-27593	An externally controlled reference to a resource vulnerability has been reported to affect QNAP NAS running Photo Station. If exploited, This could allow an attacker to modify system files. We have already fixed the vulnerability in the following versions: QTS 5.0.1: Photo Station 6.1.2 and later QTS 5.0.0/4.5.x: Photo Station 6.0.22 and later QTS 4.3.6: Photo Station 5.7.18 and later QTS 4.3.3: Photo Station 5.4.15 and later QTS 4.2.6: Photo Station 5.2.14 and later	10.0	More Details
CVE-2021-36782	A Cleartext Storage of Sensitive Information vulnerability in SUSE Rancher allows authenticated Cluster Owners, Cluster Members, Project Owners, Project Members and User Base to use the Kubernetes API to retrieve plaintext version of sensitive data. This issue affects: SUSE Rancher Rancher versions prior to 2.5.16; Rancher versions prior to 2.6.7.	9.9	More Details
CVE-2021-36783	A Insufficiently Protected Credentials vulnerability in SUSE Rancher allows authenticated Cluster Owners, Cluster Members, Project Owners and Project Members to read credentials, passwords and API tokens that have been stored in cleartext and exposed via API endpoints. This issue affects: SUSE Rancher Rancher versions prior to 2.6.4; Rancher versions prior to 2.5.13.	9.9	More Details
CVE-2022-36084	cruddl is software for creating a GraphQL API for a database, using the GraphQL SDL to model a schema. If cruddl starting with version 1.1.0 and prior to versions 2.7.0 and 3.0.2 is used to generate a schema that uses `@flexSearchFulltext`, users of that schema may be able to inject arbitrary AQL queries that will be forwarded to and executed by ArangoDB. Schemas that do not use `@flexSearchFulltext` are not affected. The attacker needs to have `READ` permission to at least one root entity type that has `@flexSearchFulltext` enabled. The issue has been fixed in version 3.0.2 and in version 2.7.0 of cruddl. As a workaround, users can temporarily remove `@flexSearchFulltext` from their schemas.	9.9	More Details
CVE-2022-36100	XWiki Platform Applications Tag and XWiki Platform Tag UI are tag applications for XWiki, a generic wiki platform. Starting with version 1.7 in XWiki Platform Applications Tag and prior to 13.10.6 and 14.4 in XWiki Platform Tag UI, the tags document `Main.Tags` in XWiki didn't sanitize user inputs properly. This allowed users with view rights on the document (default in a public wiki or for authenticated users on private wikis) to execute arbitrary Groovy, Python and Velocity code with programming rights. This also allowed bypassing all rights checks and thus both modification and disclosure of all content stored in the XWiki installation. The vulnerability could be used to impact the availability of the wiki. On XWiki versions before 13.10.4 and 14.2, this can be combined with CVE-2022-36092, meaning that no rights are required to perform the attack. The vulnerability has been patched in versions 13.10.6 and 14.4. As a workaround, the patch that fixes the issue can be manually applied to the document `Main.Tags` or the updated version of that document can be imported from version 14.4 of xwiki-platform-tag-ui using the import feature in the administration UI on XWiki 10.9 and later.	9.9	More Details

CVE Number	Description	Base Score	Reference
CVE-2022-36099	XWiki Platform Wiki UI Main Wiki is software for managing subwikis on XWiki Platform, a generic wiki platform. Starting with version 5.3-milestone-2 and prior to versions 13.10.6 and 14.4, it's possible to inject arbitrary wiki syntax including Groovy, Python and Velocity script macros via the request (URL parameter) using the `XWikiServerClassSheet` if the user has view access to this sheet and another page that has been saved with programming rights, a standard condition on a public read-only XWiki installation or a private XWiki installation where the user has an account. This allows arbitrary Groovy/Python/Velocity code execution which allows bypassing all rights checks and thus both modification and disclosure of all content stored in the XWiki installation. Also, this could be used to impact the availability of the wiki. This has been patched in versions 13.10.6 and 14.4. As a workaround, edit the affected document `XWiki.XWikiServerClassSheet` or `WikiManager.XWikiServerClassSheet` and manually perform the changes from the patch fixing the issue. On XWiki versions 12.0 and later, it is also possible to import the document `XWiki.XWikiServerClassSheet` from the xwiki-platform-wiki-ui-mainwiki package version 14.4 using the import feature of the administration application as there have been no other changes to this document since XWiki 12.0.	9.9	More Details
CVE-2022-39206	Onedev is an open source, self-hosted Git Server with CI/CD and Kanban. When using Docker-based job executors, the Docker socket (e.g. /var/run/docker.sock on Linux) is mounted into each Docker step. Users that can define and trigger CI/CD jobs on a project could use this to control the Docker daemon on the host machine. This is a known dangerous pattern, as it can be used to break out of Docker containers and, in most cases, gain root privileges on the host system. This issue allows regular (non-admin) users to potentially take over the build infrastructure of a OneDev instance. Attackers need to have an account (or be able to register one) and need permission to create a project. Since code.onedev.io has the right preconditions for this to be exploited by remote attackers, it could have been used to hijack builds of OneDev itself, e.g. by injecting malware into the docker images that are built and pushed to Docker Hub. The impact is increased by this as described before. Users are advised to upgrade to 7.3.0 or higher. There are no known workarounds for this issue.	9.9	More Details
CVE-2022-34718	Windows TCP/IP Remote Code Execution Vulnerability	9.8	More Details
CVE-2022-38297	UCMS v1.6.0 contains an authentication bypass vulnerability which is exploited via cookie poisoning.	9.8	More Details
CVE-2022-37011	A vulnerability has been identified in Mendix SAML (Mendix 7 compatible) (All versions < V1.17.0), Mendix SAML (Mendix 8 compatible) (All versions < V2.3.0), Mendix SAML (Mendix 9 compatible, New Track) (All versions < V3.3.1), Mendix SAML (Mendix 9 compatible, Upgrade Track) (All versions < V3.3.0). Affected versions of the module insufficiently protect from packet capture replay. This could allow unauthorized remote attackers to bypass authentication and get access to the application. For compatibility reasons, fix versions still contain this issue, but only when the not recommended, non default configuration option `'Allow Idp Initiated Authentication'` is enabled.	9.8	More Details
CVE-2022-38537	Archery v1.4.5 to v1.8.5 was discovered to contain multiple SQL injection vulnerabilities via the start_file, end_file, start_time, and stop_time parameters in the binlog2sql interface.	9.8	More Details
CVE-2022-38538	Archery v1.7.0 to v1.8.5 was discovered to contain a SQL injection vulnerability via the checksum parameter in the report module.	9.8	More Details
CVE-2022-38539	Archery v1.7.5 to v1.8.5 was discovered to contain a SQL injection vulnerability via the where parameter at /archive/apply.	9.8	More Details
CVE-2022-38540	Archery v1.4.0 to v1.8.5 was discovered to contain a SQL injection vulnerability via the ThreadIDs parameter in the create_kill_session interface.	9.8	More Details
CVE-2022-38541	Archery v1.8.3 to v1.8.5 was discovered to contain multiple SQL injection vulnerabilities via the start_time and stop_time parameters in the my2sql interface.	9.8	More Details
CVE-2022-38542	Archery v1.4.0 to v1.8.5 was discovered to contain a SQL injection vulnerability via the ThreadIDs parameter in the kill_session interface. The project has released an update, please upgrade to v1.9.0 and above.	9.8	More Details
CVE-2022-34721	Windows Internet Key Exchange (IKE) Protocol Extensions Remote Code Execution Vulnerability	9.8	More Details
CVE-2022-38292	SLiMS Senayan Library Management System v9.4.2 was discovered to contain multiple Server-Side Request Forgeries via the components /bibliography/marcsru.php and /bibliography/z3950sru.php.	9.8	More Details

CVE Number	Description	Base Score	Reference
CVE-2022-34722	Windows Internet Key Exchange (IKE) Protocol Extensions Remote Code Execution Vulnerability	9.8	More Details
CVE-2021-0942	The path in this case is a little bit convoluted. The end result is that via an ioctl an untrusted app can control the ui32PageIndex offset in the expression:sPA.uiAddr = page_to_phys(psOSPageArrayData->pagearray[ui32PageIndex]);With the current PoC this crashes as an OOB read. However, given that the OOB read value is ending up as the address field of a struct I think i seems plausible that this could lead to an OOB write if the attacker is able to cause the OOB read to pull an interesting kernel address. Regardless if this is a read or write, it is a High severity issue in the kernel.Product: AndroidVersions: Android SoCAndroid ID: A-238904312	9.8	More Details
CVE-2022-20385	a function called 'nla_parse', do not check the len of para, it will check nla_type (which can be controlled by userspace) with 'maxtype' (in this case, it is GSCAN_MAX), then it access polciy array 'policy[type]', which OOB access happens.Product: AndroidVersions: Android SoCAndroid ID: A-238379819	9.8	More Details
CVE-2022-20386	Summary:Product: AndroidVersions: Android SoCAndroid ID: A-238227328	9.8	More Details
CVE-2022-20387	Summary:Product: AndroidVersions: Android SoCAndroid ID: A-238227324	9.8	More Details
CVE-2022-20388	Summary:Product: AndroidVersions: Android SoCAndroid ID: A-238227323	9.8	More Details
CVE-2022-20389	Summary:Product: AndroidVersions: Android SoCAndroid ID: A-238257004	9.8	More Details
CVE-2022-20390	Summary:Product: AndroidVersions: Android SoCAndroid ID: A-238257002	9.8	More Details
CVE-2022-20391	Summary:Product: AndroidVersions: Android SoCAndroid ID: A-238257000	9.8	More Details
CVE-2022-38637	Hospital Management System v1.0 was discovered to contain multiple SQL injection vulnerabilities via the Username and Password parameters on the Login page.	9.8	More Details
CVE-2022-39815	In NOKIA 1350 OMS R14.2, multiple OS Command Injection vulnerabilities occurs. This vulnerability allow unauthenticated users to execute commands on the operating system.	9.8	More Details
CVE-2022-35413	WAPPLES through 6.0 has a hardcoded systemi account. A threat actor could use this account to access the system configuration and confidential information (such as SSL keys) via an HTTPS request to the /webapi/ URI on port 443 or 5001.	9.8	More Details
CVE-2022-38768	The mobile application in Transtek Mojodat FAM (Fixed Asset Management) 2.4.6 allows remote attackers to bypass authorization.	9.8	More Details
CVE-2022-38296	Cuppa CMS v1.0 was discovered to contain an arbitrary file upload vulnerability via the File Manager.	9.8	More Details
CVE-2022-37767	Pebble Templates 3.1.5 allows attackers to bypass a protection mechanism and implement arbitrary code execution with springbok. NOTE: the vendor disputes this because input to the Pebble templating engine is intended to include arbitrary Java code, and thus either the input should not arrive from an untrusted source, or else the application using the engine should apply restrictions to the input. The engine is not responsible for validating the input.	9.8	More Details
CVE-2022-37860	The web configuration interface of the TP-Link M7350 V3 with firmware version 190531 is affected by a pre-authentication command injection vulnerability.	9.8	More Details
CVE-2022-37300	A CWE-640: Weak Password Recovery Mechanism for Forgotten Password vulnerability exists that could cause unauthorized access in read and write mode to the controller when communicating over Modbus. Affected Products: EcoStruxure Control Expert Including all Unity Pro versions (former name of EcoStruxure Control Expert) (V15.0 SP1 and prior), EcoStruxure Process Expert, Including all versions of EcoStruxure Hybrid DCS (former name of EcoStruxure Process Expert) (V2021 and prior), Modicon M340 CPU (part numbers BMXP34*) (V3.40 and prior), Modicon M580 CPU (part numbers BMEP* and BMEH*) (V3.20 and prior).	9.8	More Details

CVE Number	Description	Base Score	Reference
CVE-2022-36587	In Tenda G3 US_G3V3.0br_V15.11.0.6(7663)_EN_TDE, there is a buffer overflow vulnerability caused by sprintf in function in the httpd binary.	9.8	More Details
CVE-2022-36660	xhyve commit dfbe09b was discovered to contain a stack buffer overflow via the component pci_vtrnd_notify().	9.8	More Details
CVE-2022-38309	Tenda AC18 router v15.03.05.19 and v15.03.05.05 was discovered to contain a stack overflow via the list parameter at /goform/SetVirtualServerCfg.	9.8	More Details
CVE-2022-38310	Tenda AC18 router v15.03.05.19 and v15.03.05.05 was discovered to contain a stack overflow via the list parameter at /goform/SetStaticRouteCfg.	9.8	More Details
CVE-2022-38311	Tenda AC18 router v15.03.05.19 and v15.03.05.05 was discovered to contain a stack overflow via the time parameter at /goform/PowerSaveSet.	9.8	More Details
CVE-2022-38312	Tenda AC18 router v15.03.05.19 and v15.03.05.05 was discovered to contain a stack overflow via the list parameter at /goform/SetIpMacBind.	9.8	More Details
CVE-2022-38313	Tenda AC18 router v15.03.05.19 and v15.03.05.05 was discovered to contain a stack overflow via the time parameter at /goform/saveParentControlInfo.	9.8	More Details
CVE-2022-38314	Tenda AC18 router v15.03.05.19 and v15.03.05.05 was discovered to contain a stack overflow via the urls parameter at /goform/saveParentControlInfo.	9.8	More Details
CVE-2022-38250	Nagios XI v5.8.6 was discovered to contain a SQL injection vulnerability via the mib_name parameter at the Manage MIBs page.	9.8	More Details
CVE-2022-36585	In Tenda G3 US_G3V3.0br_V15.11.0.6(7663)_EN_TDE, in httpd binary, the addDhcpRule function has a buffer overflow caused by sscanf.	9.8	More Details
CVE-2021-34236	Buffer Overflow in Netgear R8000 Router with firmware v1.0.4.56 allows remote attackers to execute arbitrary code or cause a denial-of-service by sending a crafted POST to '/bd_genie_create_account.cgi' with a sufficiently long parameter 'register_country'.	9.8	More Details
CVE-2022-36586	In Tenda G3 US_G3V3.0br_V15.11.0.6(7663)_EN_TDE, there is a buffer overflow vulnerability caused by strcpy in function 0x869f4 in the httpd binary.	9.8	More Details
CVE-2022-36588	In D-Link DAP1650 v1.04 firmware, the fileaccess.cgi program in the firmware has a buffer overflow vulnerability caused by strncpy.	9.8	More Details
CVE-2022-33941	PowerCMS XMLRPC API provided by Alfasado Inc. contains a command injection vulnerability. Sending a specially crafted message by POST method to PowerCMS XMLRPC API may allow arbitrary Perl script execution, and an arbitrary OS command may be executed through it. Affected products/versions are as follows: PowerCMS 6.021 and earlier (PowerCMS 6 Series), PowerCMS 5.21 and earlier (PowerCMS 5 Series), and PowerCMS 4.51 and earlier (PowerCMS 4 Series). Note that all versions of PowerCMS 3 Series and earlier which are unsupported (End-of-Life, EOL) are also affected by this vulnerability.	9.8	More Details
CVE-2022-38394	Use of hard-coded credentials for the telnet server of CentreCOM AR260S V2 firmware versions prior to Ver.3.3.7 allows a remote unauthenticated attacker to execute an arbitrary OS command.	9.8	More Details
CVE-2022-37163	Bminusl IHateToBudget v1.5.7 employs a weak password policy which allows attackers to potentially gain unauthorized access to the application via brute-force attacks. Additionally, user passwords are hashed without a salt or pepper making it much easier for tools like hashcat to crack the hashes.	9.8	More Details
CVE-2022-37164	Inoda OnTrack v3.4 employs a weak password policy which allows attackers to potentially gain unauthorized access to the application via brute-force attacks. Additionally, user passwords are hashed without a salt or pepper making it much easier for tools like hashcat to crack the hashes.	9.8	More Details
CVE-2022-40305	A Server-Side Request Forgery issue in Canto Cumulus through 11.1.3 allows attackers to enumerate the internal network, overload network resources, and possibly have unspecified other impact via the server parameter to the /cwc/login login form.	9.8	More Details
CVE-2022-2526	A use-after-free vulnerability was found in systemd. This issue occurs due to the on_stream_io() function and dns_stream_complete() function in 'resolved-dns-stream.c' not incrementing the reference counting for the DnsStream object. Therefore, other functions and callbacks called can dereference the DNSStream object, causing the use-after-free when the reference is still used later.	9.8	More Details

CVE Number	Description	Base Score	Reference
CVE-2021-44835	An issue was discovered in Active Intelligent Visualization 5. The Vdc header is used in a SQL query without being sanitized. This causes SQL injection.	9.8	More Details
CVE-2022-39135	Apache Calcite 1.22.0 introduced the SQL operators EXISTS_NODE, EXTRACT_XML, XML_TRANSFORM and EXTRACT_VALUE do not restrict XML External Entity references in their configuration, making them vulnerable to a potential XML External Entity (XXE) attack. Therefore any client exposing these operators, typically by using Oracle dialect (the first three) or MySQL dialect (the last one), is affected by this vulnerability (the extent of it will depend on the user under which the application is running). From Apache Calcite 1.32.0 onwards, Document Type Declarations and XML External Entity resolution are disabled on the impacted operators.	9.8	More Details
CVE-2022-37794	In Library Management System 1.0 the /card/in-card.php file id_no parameters are vulnerable to SQL injection.	9.8	More Details
CVE-2022-38771	The mobile application in Transtek Mojodat FAM (Fixed Asset Management) 2.4.6 allows remote attackers to send SCRIPT tags as injected input to the API request.	9.8	More Details
CVE-2022-38638	Casdoor v1.97.3 was discovered to contain an arbitrary file write vulnerability via the fullFilePath parameter at /api/upload-resource.	9.1	More Details
CVE-2022-31247	An Improper Authorization vulnerability in SUSE Rancher, allows any user who has permissions to create/edit cluster role template bindings or project role template bindings (such as cluster-owner, manage cluster members, project-owner and manage project members) to gain owner permission in another project in the same cluster or in another project on a different downstream cluster. This issue affects: SUSE Rancher Rancher versions prior to 2.6.7; Rancher versions prior to 2.5.16.	9.1	More Details
CVE-2022-39205	Onedev is an open source, self-hosted Git Server with CI/CD and Kanban. In versions of Onedev prior to 7.3.0 unauthenticated users can take over a OneDev instance if there is no properly configured reverse proxy. The /git-prereceive-callback endpoint is used by the pre-receive git hook on the server to check for branch protections during a push event. It is only intended to be accessed from localhost, but the check relies on the X-Forwarded-For header. Invoking this endpoint leads to the execution of one of various git commands. The environment variables of this command execution can be controlled via query parameters. This allows attackers to write to arbitrary files, which can in turn lead to the execution of arbitrary code. Such an attack would be very hard to detect, which increases the potential impact even more. Users are advised to upgrade. There are no known workarounds for this issue.	9.0	More Details

OTHER VULNERABILITIES

CVE Number	Description	Base Score	Reference
CVE-2022-36096	The XWiki Platform Index UI is an Index of all pages, attachments, orphans and deleted pages and attachments for XWiki Platform, a generic wiki platform. Prior to versions 13.10.6 and 14.3, it's possible to store JavaScript which will be executed by anyone viewing the deleted attachments index with an attachment containing javascript in its name. This issue has been patched in XWiki 13.10.6 and 14.3. As a workaround, modify fix the vulnerability by editing the wiki page `XWiki.DeletedAttachments` with the object editor, open the `JavaScriptExtension` object and apply on the content the changes that can be found on the fix commit.	8.9	More Details
CVE-2022-36097	XWiki Platform Attachment UI provides a macro to easily upload and select attachments for XWiki Platform, a generic wiki platform. Starting with version 14.0-rc-1 and prior to 14.4-rc-1, it's possible to store JavaScript in an attachment name, which will be executed by anyone trying to move the corresponding attachment. This issue has been patched in XWiki 14.4-rc-1. As a workaround, one may copy `moveStep1.vm` to `webapp/xwiki/templates/moveStep1.vm` and replace vulnerable code with code from the patch.	8.9	More Details
CVE-2022-36098	XWiki Platform Mentions UI is a user interface for mentioning users in wiki content for XWiki Platform, a generic wiki platform. Starting in version 12.5-rc-1 and prior to versions 13.10.6 and 14.4, it's possible to store Javascript or groovy scripts in a mention, macro anchor, or reference field. The stored code is executed by anyone visiting the page with the mention. This issue has been patched on XWiki 14.4 and 13.10.6. As a workaround, one may update `XWiki.Mentions.MentionsMacro` and edit the `Macro code` field of the `XWiki.WikiMacroClass` XObject.	8.9	More Details

CVE Number	Description	Base Score	Reference
CVE-2022-36094	XWiki Platform Web Parent POM contains Web resources for the XWiki platform, a generic wiki platform. Starting with version 1.0 and prior to versions 13.10.6 and 14.30-rc-1, it's possible to store JavaScript which will be executed by anyone viewing the history of an attachment containing javascript in its name. This issue has been patched in XWiki 13.10.6 and 14.3RC1. As a workaround, it is possible to replace `viewattachrev.vm`, the entry point for this attack, by a patched version from the patch without updating XWiki.	8.9	More Details
CVE-2022-34102	Insufficient access control vulnerability was discovered in the Crestron AirMedia Windows Application, version 4.3.1.39, in which a user can pause the uninstallation of an executable to gain a SYSTEM level command prompt.	8.8	More Details
CVE-2022-40320	cfg_tilde_expand in confuse.c in libConfuse 3.3 has a heap-based buffer over-read.	8.8	More Details
CVE-2022-3167	Improper Restriction of Rendered UI Layers or Frames in GitHub repository ikus060/rdiffweb prior to 2.4.1.	8.8	More Details
CVE-2022-38305	AeroCMS v0.0.1 was discovered to contain an arbitrary file upload vulnerability via the component /admin/profile.php. This vulnerability allows attackers to execute arbitrary code via a crafted PHP file.	8.8	More Details
CVE-2022-35805	Microsoft Dynamics CRM (on-premises) Remote Code Execution Vulnerability	8.8	More Details
CVE-2021-44426	An issue was discovered in AnyDesk before 6.2.6 and 6.3.x before 6.3.5. An upload of an arbitrary file to a victim's local ~/Downloads/ directory is possible if the victim is using the AnyDesk Windows client to connect to a remote machine, if an attacker is also connected remotely with AnyDesk to the same remote machine. The upload is done without any approval or action taken by the victim.	8.8	More Details
CVE-2022-37190	CuppaCMS 1.0 is vulnerable to Remote Code Execution (RCE). An authenticated user can control both parameters (action and function) from "/api/index.php.	8.8	More Details
CVE-2022-34734	Microsoft ODBC Driver Remote Code Execution Vulnerability	8.8	More Details
CVE-2022-38615	SmartVista SVFE2 v2.2.22 was discovered to contain multiple SQL injection vulnerabilities via the UserForm:j_id88, UserForm:j_id90, and UserForm:j_id92 parameters at /SVFE2/pages/feegroups/service_group.jsf.	8.8	More Details
CVE-2022-35841	Windows Enterprise App Management Service Remote Code Execution Vulnerability	8.8	More Details
CVE-2022-36110	Netmaker makes networks with WireGuard. Prior to version 0.15.1, Improper Authorization functions lead to non-privileged users running privileged API calls. If someone adds users to the Netmaker platform who do not have admin privileges, they can use their auth tokens to run admin-level functions via the API. This problem has been patched in v0.15.1.	8.8	More Details
CVE-2022-37961	Microsoft SharePoint Server Remote Code Execution Vulnerability	8.8	More Details
CVE-2022-38616	SmartVista SVFE2 v2.2.22 was discovered to contain a SQL injection vulnerability via the UserForm:j_id90 parameter at /feegroups/tgrt_group.jsf.	8.8	More Details
CVE-2022-38531	FPT G-97RG6M R4.2.98.035 and G-97RG3 R4.2.43.078 are vulnerable to Remote Command Execution in the ping function.	8.8	More Details

CVE Number	Description	Base Score	Reference
CVE-2022-37144	The PlexTrac platform prior to API version 1.17.0 does not restrict excessive MFA TOTP submission attempts. An unauthenticated remote attacker in possession of a valid username and password can bruteforce their way past MFA protections to login as the targeted user.	8.8	More Details
CVE-2022-34726	Microsoft ODBC Driver Remote Code Execution Vulnerability	8.8	More Details
CVE-2022-35582	Penta Security Systems Inc WAPPLES 4.0.*, 5.0.0.*, 5.0.12.* are vulnerable to Incorrect Access Control. The operating system that WAPPLES runs on has a built-in non-privileged user penta with a predefined password. The password for this user, as well as its existence, is not disclosed in the documentation. Knowing the credentials, attackers can use this feature to gain uncontrolled access to the device and therefore are considered an undocumented possibility for remote control.	8.8	More Details
CVE-2022-34733	Microsoft WDAC OLE DB provider for SQL Server Remote Code Execution Vulnerability	8.8	More Details
CVE-2022-34732	Microsoft ODBC Driver Remote Code Execution Vulnerability	8.8	More Details
CVE-2022-34727	Microsoft ODBC Driver Remote Code Execution Vulnerability	8.8	More Details
CVE-2022-34869	Undocumented hidden command that can be executed from the telnet function of CentreCOM AR260S V2 firmware versions prior to Ver.3.3.7 allows a remote authenticated attacker to execute an arbitrary OS command.	8.8	More Details
CVE-2022-35273	OS command injection vulnerability in GUI setting page of CentreCOM AR260S V2 firmware versions prior to Ver.3.3.7 allows a remote authenticated attacker to execute an arbitrary OS command.	8.8	More Details
CVE-2022-30079	Command injection vulnerability was discovered in Netgear R6200 v2 firmware through R6200v2-V1.0.3.12 via binary /sbin/acos_service that could allow remote authenticated attackers the ability to modify values in the vulnerable parameter.	8.8	More Details
CVE-2022-38094	OS command injection vulnerability in the telnet function of CentreCOM AR260S V2 firmware versions prior to Ver.3.3.7 allows a remote authenticated attacker to execute an arbitrary OS command.	8.8	More Details
CVE-2022-35823	Microsoft SharePoint Remote Code Execution Vulnerability	8.8	More Details
CVE-2022-40623	The WAVLINK Quantum D4G (WN531G3) running firmware version M31G3.V5030.200325 does not utilize anti-CSRF tokens, which, when combined with other issues (such as CVE-2022-35518), can lead to remote, unauthenticated command execution.	8.8	More Details
CVE-2022-34731	Microsoft WDAC OLE DB provider for SQL Server Remote Code Execution Vulnerability	8.8	More Details
CVE-2022-34700	Microsoft Dynamics CRM (on-premises) Remote Code Execution Vulnerability	8.8	More Details
CVE-2022-39817	In NOKIA 1350 OMS R14.2, multiple SQL Injection vulnerabilities occurs. Exploitation requires an authenticated attacker. Through the injection of arbitrary SQL statements, a potential authenticated attacker can modify query syntax and perform unauthorized (and unexpected) operations against the remote database.	8.8	More Details
CVE-2022-34100	A vulnerability was discovered in the Crestron AirMedia Windows Application, version 4.3.1.39, in which a low-privileged user can gain a SYSTEM level command prompt by pre-staging a file structure prior to the installation of a trusted service executable and change permissions on that file structure during a repair operation.	8.8	More Details

CVE Number	Description	Base Score	Reference
CVE-2022-31149	ActivityWatch open-source automated time tracker. Versions prior to 0.12.0b2 are vulnerable to DNS rebinding attacks. This vulnerability impacts everyone running ActivityWatch and gives the attacker full access to the ActivityWatch REST API. Users should upgrade to v0.12.0b2 or later to receive a patch. As a workaround, block DNS lookups that resolve to 127.0.0.1.	8.8	More Details
CVE-2022-39819	In NOKIA 1350 OMS R14.2, multiple OS Command Injection vulnerabilities occurs. This allows authenticated users to execute commands on the operating system.	8.8	More Details
CVE-2022-35835	Microsoft WDAC OLE DB provider for SQL Server Remote Code Execution Vulnerability	8.8	More Details
CVE-2022-32555	Unisys Data Exchange Management Studio before 6.0.IC2 and 7.x before 7.0.IC1 doesn't have an Anti-CSRF token to authenticate the POST request. Thus, a cross-site request forgery attack could occur.	8.8	More Details
CVE-2022-35836	Microsoft WDAC OLE DB provider for SQL Server Remote Code Execution Vulnerability	8.8	More Details
CVE-2022-37730	In ftcms 2.1, there is a Cross Site Request Forgery (CSRF) vulnerability in the PHP page, which causes the attacker to forge a link to trick him to click on a malicious link or visit a page containing attack code, and send a request to the server (corresponding to the identity authentication information) as the victim without the victim's knowledge.	8.8	More Details
CVE-2022-3179	Weak Password Requirements in GitHub repository ikus060/rdiffweb prior to 2.4.2.	8.8	More Details
CVE-2022-3152	Unverified Password Change in GitHub repository phpfusion/phpfusion prior to 9.10.20.	8.8	More Details
CVE-2022-39203	matrix-appservice-irc is an open source Node.js IRC bridge for Matrix. Attackers can specify a specific string of characters, which would confuse the bridge into combining an attacker-owned channel and an existing channel, allowing them to grant themselves permissions in the channel. The vulnerability has been patched in matrix-appservice-irc 0.35.0. As a workaround operators may disable dynamic channel joining via `dynamicChannels.enabled` to prevent users from joining new channels, which prevents any new channels being bridged outside of what is already bridged, and what is specified in the config.	8.8	More Details
CVE-2022-40622	The WAVLINK Quantum D4G (WN531G3) running firmware version M31G3.V5030.200325 uses IP addresses to hold sessions and does not not use session tokens. Therefore, if an attacker changes their IP address to match the logged-in administrator's, or is behind the same NAT as the logged in administrator, session takeover is possible.	8.8	More Details
CVE-2022-38009	Microsoft SharePoint Server Remote Code Execution Vulnerability	8.8	More Details
CVE-2022-38008	Microsoft SharePoint Server Remote Code Execution Vulnerability	8.8	More Details
CVE-2022-35834	Microsoft WDAC OLE DB provider for SQL Server Remote Code Execution Vulnerability	8.8	More Details
CVE-2022-38144	Cross-Site Request Forgery (CSRF) vulnerability in gVectors Team wpForo Forum plugin <= 2.0.5 at WordPress.	8.8	More Details
CVE-2022-30078	NETGEAR R6200_V2 firmware versions through R6200v2-V1.0.3.12_10.1.11 and R6300_V2 firmware versions through R6300v2-V1.0.4.52_10.0.93 allow remote authenticated attackers to execute arbitrary command via shell metacharacters in the ipv6_fix.cgi ipv6_wan_ipaddr, ipv6_lan_ipaddr, ipv6_wan_length, or ipv6_lan_length parameters.	8.8	More Details

CVE Number	Description	Base Score	Reference
CVE-2022-38700	OpenHarmony-v3.1.1 and prior versions have a permission bypass vulnerability. LAN attackers can bypass permission control and get control of camera service.	8.8	More Details
CVE-2022-38298	Appsmith v1.7.11 was discovered to allow attackers to execute an authenticated Server-Side Request Forgery (SSRF) via redirecting incoming requests to the AWS internal metadata endpoint.	8.8	More Details
CVE-2022-35840	Microsoft WDAC OLE DB provider for SQL Server Remote Code Execution Vulnerability	8.8	More Details
CVE-2022-34730	Microsoft ODBC Driver Remote Code Execution Vulnerability	8.8	More Details
CVE-2022-37108	An injection vulnerability in the syslog-ng configuration wizard in Securonix Snypr 6.4 allows an application user with the "Manage Ingesters" permission to execute arbitrary code on remote ingesters by appending arbitrary text to text files that are executed by the system, such as users' crontab files. The patch for this was present in SNYPR version 6.4 Jun 2022 R3_[06170871], but may have been introduced sooner.	8.7	More Details
CVE-2022-36079	Parse Server is an open source backend that can be deployed to any infrastructure that can run Node.js. Internal fields (keys used internally by Parse Server, prefixed by `_`) and protected fields (user defined) can be used as query constraints. Internal and protected fields are removed by Parse Server and are only returned to the client using a valid master key. However, using query constraints, these fields can be guessed by enumerating until Parse Server, prior to versions 4.10.14 or 5.2.5, returns a response object. The patch available in versions 4.10.14 and 5.2.5 requires the maser key to use internal and protected fields as query constraints. As a workaround, implement a Parse Cloud Trigger `beforeFind` and manually remove the query constraints.	8.6	More Details
CVE-2022-36093	XWiki Platform Web Templates are templates for XWiki Platform, a generic wiki platform. By passing a template of the distribution wizard to the xpart template, user accounts can be created even when user registration is disabled. This also circumvents any email verification. Before versions 14.2 and 13.10.4, this can also be exploited on a private wiki, thus potentially giving the attacker access to the wiki. Depending on the configured default rights of users, this could also give attackers write access to an otherwise read-only public wiki. Users can also be created when an external authentication system like LDAP is configured, but authentication fails unless the authentication system supports a bypass/local accounts are enabled in addition to the external authentication system. This issue has been patched in XWiki 13.10.5 and 14.3RC1. As a workaround, one may replace `xpart.vm`, the entry point for this attack, by a patched version from the patch without updating XWiki.	8.5	More Details
CVE-2022-38342	Safe Software FME Server v2021.2.5, v2022.0.0.2 and below was discovered to contain a XML External Entity (XXE) vulnerability which allows authenticated attackers to perform data exfiltration or Server-Side Request Forgery (SSRF) attacks.	8.5	More Details
CVE-2022-29490	Improper Authorization vulnerability exists in the Workplace X WebUI of the Hitachi Energy MicroSCADA X SYS600 allows an authenticated user to execute any MicroSCADA internal scripts irrespective of the authenticated user's role. This issue affects: Hitachi Energy MicroSCADA X SYS600 version 10 to version 10.3.1. cpe:2.3:a:hitachienergy:microscada_x_sys600:10:*:*:*:*:*:*:* cpe:2.3:a:hitachienergy:microscada_x_sys600:10.1:*:*:*:*:*:*:* cpe:2.3:a:hitachienergy:microscada_x_sys600:10.1.1:*:*:*:*:*:*:* cpe:2.3:a:hitachienergy:microscada_x_sys600:10.2:*:*:*:*:*:*:* cpe:2.3:a:hitachienergy:microscada_x_sys600:10.2.1:*:*:*:*:*:*:* cpe:2.3:a:hitachienergy:microscada_x_sys600:10.3:*:*:*:*:*:*:* cpe:2.3:a:hitachienergy:microscada_x_sys600:10.3.1:*:*:*:*:*:*:*	8.5	More Details
CVE-2022-36086	linked_list_allocator is an allocator usable for no_std systems. Prior to version 0.10.2, the heap initialization methods were missing a minimum size check for the given heap size argument. This could lead to out-of-bound writes when a heap was initialized with a size smaller than `3 * size_of::<usize>` because of metadata write operations. This vulnerability impacts all the initialization functions on the `Heap` and `LockedHeap` types, including `Heap::new`, `Heap::init`, `Heap::init_from_slice`, and `LockedHeap::new`. It also affects multiple uses of the `Heap::extend` method. Version 0.10.2 contains a patch for the issue. As a workaround, ensure that the heap is only initialized with a size larger than `3 * size_of::<usize>` and that the `Heap::extend` method is only called with sizes larger than `2 * size_of::<usize>()`. Also, ensure that the total heap size is (and stays) a multiple of `2 * size_of::<usize>()`.	8.4	More Details

CVE Number	Description	Base Score	Reference
CVE-2022-36073	RubyGems.org is the Ruby community gem host. A bug in password & email change confirmation code allowed an attacker to change their RubyGems.org account's email to an unowned email address. Having access to an account whose email has been changed could enable an attacker to save API keys for that account, and when a legitimate user attempts to create an account with their email (and has to reset password to gain access) and is granted access to other gems, the attacker would then be able to publish and yank versions of those gems. Commit number 90c9e6aac2d91518b479c51d48275c57de492d4d contains a patch for this issue.	8.3	More Details
CVE-2022-30196	Windows Secure Channel Denial of Service Vulnerability	8.2	More Details
CVE-2022-36089	KubeVela is an application delivery platform Users using KubeVela's VelaUX APIServer could be affected by an authentication bypass vulnerability. In KubeVela prior to versions 1.4.11 and 1.5.4, VelaUX APIServer uses the `PlatformID` as the signed key to generate the JWT tokens for users. Another API called `getSystemInfo` exposes the platformID. This vulnerability allows users to use the platformID to re-generate the JWT tokens to bypass the authentication. Versions 1.4.11 and 1.5.4 contain a patch for this issue.	8.2	More Details
CVE-2022-37958	SPNEGO Extended Negotiation (NEGOEX) Security Mechanism Remote Code Execution Vulnerability	8.1	More Details
CVE-2022-35830	Remote Procedure Call Runtime Remote Code Execution Vulnerability	8.1	More Details
CVE-2022-36174	FreshService Windows Agent < 2.11.0 and FreshService macOS Agent < 4.2.0 and FreshService Linux Agent < 3.3.0. are vulnerable to Broken integrity checking via the FreshAgent client and scheduled update service.	8.1	More Details
CVE-2022-36173	FreshService macOS Agent < 4.4.0 and FreshServce Linux Agent < 3.4.0 are vulnerable to TLS Man-in-The-Middle via the FreshAgent client and scheduled update service.	8.1	More Details
CVE-2022-38258	A local file inclusion (LFI) vulnerability in D-Link DIR 819 v1.06 allows attackers to cause a Denial of Service (DoS) or access sensitive server information via manipulation of the getpage parameter in a crafted web request.	8.1	More Details
CVE-2022-28741	aEnrich a+HRD 5.x Learning Management Key Performance Indicator System has a local file inclusion (LFI) vulnerability that occurs due to missing input validation in v5.x	8.1	More Details
CVE-2022-33647	Windows Kerberos Elevation of Privilege Vulnerability	8.1	More Details
CVE-2022-36090	XWiki Platform Old Core is a core package for XWiki Platform, a generic wiki platform. Prior to versions 13.1.0.5 and 14.3-rc-1, some resources are missing a check for inactive (not yet activated or disabled) users in XWiki, including the REST service. This means a disabled user can enable themselves using a REST call. On the same way some resources handler created by extensions are not protected by default, so an inactive user could perform actions for such extensions. This issue has existed since at least version 1.1 of XWiki for instance configured with the email activation required for new users. Now it's more critical for versions 11.3-rc-1 and later since the maintainers provided the capability to disable user without deleting them and encouraged using that feature. XWiki 14.3-rc-1 and XWiki 13.10.5 contain a patch. There is no workaround for this other than upgrading XWiki.	8.1	More Details
CVE-2022-31166	XWiki Platform Old Core is a core package for XWiki Platform, a generic wiki platform. Starting in versions 11.3.7, 11.0.3, and 12.0RC1, it is possible to exploit a bug in XWikiRights resolution of groups to obtain privilege escalation. More specifically, editing a right with the object editor leads to adding a supplementary empty value to groups which is then resolved as a reference to XWiki.WebHome page. Adding an XWikiGroup xobject to that page then transforms it to a group, any user put in that group would then obtain the privileges related to the edited right. Note that this security issue is normally mitigated by the fact that XWiki.WebHome (and XWiki space in general) should be protected by default for edit rights. The problem has been patched in XWiki 13.10.4 and 14.2RC1 to not consider anymore empty values in XWikiRights. It's possible to work around the problem by setting appropriate rights on XWiki.WebHome page to prevent users to edit it.	8.1	More Details

CVE Number	Description	Base Score	Reference
CVE-2022-33679	Windows Kerberos Elevation of Privilege Vulnerability	8.1	More Details
CVE-2022-36768	IBM AIX 7.1, 7.2, 7.3, and VIOS 3.1 could allow a non-privileged local user to exploit a vulnerability in the invscout command to obtain root privileges. IBM X-Force ID: 232014.	7.8	More Details
CVE-2022-20395	In checkAccess of MediaProvider.java, there is a possible file deletion due to a path traversal error. This could lead to local escalation of privilege with no additional execution privileges needed. User interaction is not needed for exploitation.Product: AndroidVersions: Android-11 Android-12 Android-12L Android-13Android ID: A-221855295	7.8	More Details
CVE-2022-38010	Microsoft Office Visio Remote Code Execution Vulnerability	7.8	More Details
CVE-2022-38019	AV1 Video Extension Remote Code Execution Vulnerability	7.8	More Details
CVE-2022-39141	A vulnerability has been identified in Parasolid V33.1 (All versions < V33.1.262), Parasolid V34.0 (All versions < V34.0.252), Parasolid V34.1 (All versions < V34.1.242), Parasolid V35.0 (All versions < V35.0.161), Simcenter Femap V2022.1 (All versions < V2022.1.3), Simcenter Femap V2022.2 (All versions < V2022.2.2). The affected application is vulnerable to out of bounds read past the end of an allocated buffer when parsing X_T files. An attacker could leverage this vulnerability to leak information in the context of the current process. (ZDI-CAN-17296)	7.8	More Details
CVE-2022-3170	An out-of-bounds access issue was found in the Linux kernel sound subsystem. It could occur when the 'id->name' provided by the user did not end with '\0'. A privileged local user could pass a specially crafted name through ioctl() interface and crash the system or potentially escalate their privileges on the system.	7.8	More Details
CVE-2021-0871	In PVRSRVBridgePMRPDumpSymbolicAddr of the PowerVR kernel driver, a missing size check means there is a possible integer overflow that could allow out-of-bounds heap access. This could lead to local escalation of privilege with no additional execution privileges needed. User interaction is not needed for exploitation.Product: AndroidVersions: Android SoCAndroid ID: A-238921253	7.8	More Details
CVE-2021-0943	In MMU_MapPages of TBD, there is a possible out of bounds write due to improper input validation. This could lead to local escalation of privilege with no additional execution privileges needed. User interaction is not needed for exploitation.Product: AndroidVersions: Android SoCAndroid ID: A-238916921	7.8	More Details
CVE-2022-20392	In declareDuplicatePermission of ParsedPermissionUtils.java, there is a possible way to obtain a dangerous permission without user consent due to improper input validation. This could lead to local escalation of privilege during app installation or upgrade with no additional execution privileges needed. User interaction is not needed for exploitation.Product: AndroidVersions: Android-10 Android-11 Android-12 Android-12LAndroid ID: A-213323615	7.8	More Details
CVE-2022-39146	A vulnerability has been identified in Parasolid V33.1 (All versions < V33.1.262), Parasolid V33.1 (All versions >= V33.1.262 < V33.1.263), Parasolid V34.0 (All versions < V34.0.252), Parasolid V34.1 (All versions < V34.1.242), Parasolid V35.0 (All versions < V35.0.161), Parasolid V35.0 (All versions >= V35.0.161 < V35.0.164), Simcenter Femap V2022.1 (All versions < V2022.1.3), Simcenter Femap V2022.2 (All versions < V2022.2.2). The affected application is vulnerable to uninitialized pointer access while parsing specially crafted X_T files. An attacker could leverage this vulnerability to execute code in the context of the current process. (ZDI-CAN-17502)	7.8	More Details
CVE-2022-39142	A vulnerability has been identified in Parasolid V33.1 (All versions < V33.1.262), Parasolid V33.1 (All versions >= V33.1.262 < V33.1.263), Parasolid V34.0 (All versions < V34.0.252), Parasolid V34.1 (All versions < V34.1.242), Parasolid V35.0 (All versions < V35.0.161), Parasolid V35.0 (All versions >= V35.0.161 < V35.0.164), Simcenter Femap V2022.1 (All versions < V2022.1.3), Simcenter Femap V2022.2 (All versions < V2022.2.2). The affected application contains an out of bounds write past the end of an allocated buffer while parsing specially crafted X_T files. This could allow an attacker to execute code in the context of the current process. (ZDI-CAN-17485)	7.8	More Details
CVE-2022-20398	In addOrUpdateNetwork of WifiServiceImpl.java, there is a possible way for a guest user to configure Wi-Fi due to a permissions bypass. This could lead to local escalation of privilege with User execution privileges needed. User interaction is not needed for exploitation.Product: AndroidVersions: Android-13Android ID: A-221859734	7.8	More Details

CVE Number	Description	Base Score	Reference
CVE-2022-38306	LIEF commit 5d1d643 was discovered to contain a heap-buffer overflow in the component /core/CorePrPsInfo.tcc.	7.8	More Details
CVE-2022-39145	A vulnerability has been identified in Parasolid V33.1 (All versions < V33.1.262), Parasolid V33.1 (All versions >= V33.1.262 < V33.1.263), Parasolid V34.0 (All versions < V34.0.252), Parasolid V34.1 (All versions < V34.1.242), Parasolid V35.0 (All versions < V35.0.161), Parasolid V35.0 (All versions >= V35.0.161 < V35.0.164), Simcenter Femap V2022.1 (All versions < V2022.1.3), Simcenter Femap V2022.2 (All versions < V2022.2.2). The affected application is vulnerable to out of bounds read past the end of an allocated buffer when parsing X_T files. This could allow an attacker to execute code in the context of the current process. (ZDI-CAN-17496)	7.8	More Details
CVE-2022-2962	A DMA reentrancy issue was found in the Tulip device emulation in QEMU. When Tulip reads or writes to the rx/tx descriptor or copies the rx/tx frame, it doesn't check whether the destination address is its own MMIO address. This can cause the device to trigger MMIO handlers multiple times, possibly leading to a stack or heap overflow. A malicious guest could use this flaw to crash the QEMU process on the host, resulting in a denial of service condition.	7.8	More Details
CVE-2022-38495	LIEF commit 365a16a was discovered to contain a heap-buffer overflow via the function print_binary at /c/macho_reader.c.	7.8	More Details
CVE-2022-39139	A vulnerability has been identified in Parasolid V33.1 (All versions < V33.1.262), Parasolid V34.0 (All versions < V34.0.252), Parasolid V34.1 (All versions < V34.1.242), Parasolid V35.0 (All versions < V35.0.161), Simcenter Femap V2022.1 (All versions < V2022.1.3), Simcenter Femap V2022.2 (All versions < V2022.2.2). The affected application contains an out of bounds write past the end of an allocated buffer while parsing specially crafted X_T files. This could allow an attacker to execute code in the context of the current process. (ZDI-CAN-17289)	7.8	More Details
CVE-2022-39143	A vulnerability has been identified in Parasolid V33.1 (All versions < V33.1.262), Parasolid V33.1 (All versions >= V33.1.262 < V33.1.263), Parasolid V34.0 (All versions < V34.0.252), Parasolid V34.1 (All versions < V34.1.242), Parasolid V35.0 (All versions < V35.0.161), Parasolid V35.0 (All versions >= V35.0.161 < V35.0.164), Simcenter Femap V2022.1 (All versions < V2022.1.3), Simcenter Femap V2022.2 (All versions < V2022.2.2). The affected application contains an out of bounds write past the end of an allocated buffer while parsing specially crafted X_T files. This could allow an attacker to execute code in the context of the current process. (ZDI-CAN-17493)	7.8	More Details
CVE-2022-26929	.NET Framework Remote Code Execution Vulnerability	7.8	More Details
CVE-2022-39148	A vulnerability has been identified in Parasolid V33.1 (All versions < V33.1.262), Parasolid V33.1 (All versions >= V33.1.262 < V33.1.263), Parasolid V34.0 (All versions < V34.0.252), Parasolid V34.1 (All versions < V34.1.242), Parasolid V35.0 (All versions < V35.0.161), Parasolid V35.0 (All versions >= V35.0.161 < V35.0.164), Simcenter Femap V2022.1 (All versions < V2022.1.3), Simcenter Femap V2022.2 (All versions < V2022.2.2). The affected application contains an out of bounds write past the end of an allocated buffer while parsing specially crafted X_T files. This could allow an attacker to execute code in the context of the current process. (ZDI-CAN-17513)	7.8	More Details
CVE-2022-39144	A vulnerability has been identified in Parasolid V33.1 (All versions < V33.1.262), Parasolid V33.1 (All versions >= V33.1.262 < V33.1.263), Parasolid V34.0 (All versions < V34.0.252), Parasolid V34.1 (All versions < V34.1.242), Parasolid V35.0 (All versions < V35.0.161), Parasolid V35.0 (All versions >= V35.0.161 < V35.0.164), Simcenter Femap V2022.1 (All versions < V2022.1.3), Simcenter Femap V2022.2 (All versions < V2022.2.2). The affected application contains an out of bounds write past the end of an allocated buffer while parsing specially crafted X_T files. This could allow an attacker to execute code in the context of the current process. (ZDI-CAN-17494)	7.8	More Details
CVE-2022-34356	IBM AIX 7.1, 7.2, 7.3, and VIOS 3.1 could allow a non-privileged local user to exploit a vulnerability in the AIX kernel to obtain root privileges. IBM X-Force ID: 230502.	7.8	More Details
CVE-2022-39140	A vulnerability has been identified in Parasolid V33.1 (All versions < V33.1.262), Parasolid V34.0 (All versions < V34.0.252), Parasolid V34.1 (All versions < V34.1.242), Parasolid V35.0 (All versions < V35.0.161), Simcenter Femap V2022.1 (All versions < V2022.1.3), Simcenter Femap V2022.2 (All versions < V2022.2.2). The affected application contains an out of bounds write past the end of an allocated buffer while parsing specially crafted X_T files. This could allow an attacker to execute code in the context of the current process. (ZDI-CAN-17292)	7.8	More Details

CVE Number	Description	Base Score	Reference
CVE-2022-39154	A vulnerability has been identified in Parasolid V33.1 (All versions < V33.1.262), Parasolid V33.1 (All versions >= V33.1.262 < V33.1.263), Parasolid V34.0 (All versions < V34.0.252), Parasolid V34.1 (All versions < V34.1.242), Parasolid V35.0 (All versions < V35.0.161), Parasolid V35.0 (All versions >= V35.0.161 < V35.0.164), Simcenter Femap V2022.1 (All versions < V2022.1.3), Simcenter Femap V2022.2 (All versions < V2022.2.2). The affected application contains an out of bounds write past the end of an allocated buffer while parsing specially crafted X_T files. This could allow an attacker to execute code in the context of the current process. (ZDI-CAN-18188)	7.8	More Details
CVE-2022-39138	A vulnerability has been identified in Parasolid V33.1 (All versions < V33.1.262), Parasolid V34.0 (All versions < V34.0.252), Parasolid V34.1 (All versions < V34.1.242), Parasolid V35.0 (All versions < V35.0.161), Simcenter Femap V2022.1 (All versions < V2022.1.3), Simcenter Femap V2022.2 (All versions < V2022.2.2). The affected application contains an out of bounds write past the end of an allocated buffer while parsing specially crafted X_T files. This could allow an attacker to execute code in the context of the current process. (ZDI-CAN-17284)	7.8	More Details
CVE-2022-39153	A vulnerability has been identified in Parasolid V33.1 (All versions < V33.1.262), Parasolid V33.1 (All versions >= V33.1.262 < V33.1.263), Parasolid V34.0 (All versions < V34.0.252), Parasolid V34.1 (All versions < V34.1.242), Parasolid V35.0 (All versions < V35.0.161), Parasolid V35.0 (All versions >= V35.0.161 < V35.0.164), Simcenter Femap V2022.1 (All versions < V2022.1.3), Simcenter Femap V2022.2 (All versions < V2022.2.2). The affected application is vulnerable to out of bounds read past the end of an allocated buffer when parsing X_T files. This could allow an attacker to execute code in the context of the current process. (ZDI-CAN-18187)	7.8	More Details
CVE-2022-3178	Buffer Over-read in GitHub repository gpac/gpac prior to 2.1.0-DEV.	7.8	More Details
CVE-2022-39156	A vulnerability has been identified in Parasolid V33.1 (All versions < V33.1.262), Parasolid V33.1 (All versions >= V33.1.262 < V33.1.263), Parasolid V34.0 (All versions < V34.0.252), Parasolid V34.1 (All versions < V34.1.242), Parasolid V35.0 (All versions < V35.0.161), Parasolid V35.0 (All versions >= V35.0.161 < V35.0.164), Simcenter Femap V2022.1 (All versions < V2022.1.3), Simcenter Femap V2022.2 (All versions < V2022.2.2). The affected application is vulnerable to out of bounds read past the end of an allocated buffer when parsing X_T files. This could allow an attacker to execute code in the context of the current process. (ZDI-CAN-18196)	7.8	More Details
CVE-2022-30200	Windows Lightweight Directory Access Protocol (LDAP) Remote Code Execution Vulnerability	7.8	More Details
CVE-2022-37956	Windows Kernel Elevation of Privilege Vulnerability	7.8	More Details
CVE-2022-37964	Windows Kernel Elevation of Privilege Vulnerability	7.8	More Details
CVE-2022-37955	Windows Group Policy Elevation of Privilege Vulnerability	7.8	More Details
CVE-2022-37963	Microsoft Office Visio Remote Code Execution Vulnerability	7.8	More Details
CVE-2022-37962	Microsoft PowerPoint Remote Code Execution Vulnerability	7.8	More Details
CVE-2022-37969	Windows Common Log File System Driver Elevation of Privilege Vulnerability	7.8	More Details
CVE-2022-3133	OS Command Injection in GitHub repository jgraph/drawio prior to 20.3.0.	7.8	More Details

CVE Number	Description	Base Score	Reference
CVE-2022-37954	DirectX Graphics Kernel Elevation of Privilege Vulnerability	7.8	More Details
CVE-2022-38004	Windows Fax Service Remote Code Execution Vulnerability	7.8	More Details
CVE-2022-39137	A vulnerability has been identified in Parasolid V33.1 (All versions < V33.1.262), Parasolid V34.0 (All versions < V34.0.252), Parasolid V34.1 (All versions < V34.1.242), Parasolid V35.0 (All versions < V35.0.161), Simcenter Femap V2022.1 (All versions < V2022.1.3), Simcenter Femap V2022.2 (All versions < V2022.2.2). The affected application is vulnerable to out of bounds read past the end of an allocated buffer when parsing X_T files. An attacker could leverage this vulnerability to leak information in the context of the current process. (ZDI-CAN-17276)	7.8	More Details
CVE-2022-2979	Opening a specially crafted file could cause the affected product to fail to release its memory reference potentially resulting in arbitrary code execution.	7.8	More Details
CVE-2022-39152	A vulnerability has been identified in Parasolid V33.1 (All versions < V33.1.262), Parasolid V33.1 (All versions >= V33.1.262 < V33.1.263), Parasolid V34.0 (All versions < V34.0.252), Parasolid V34.1 (All versions < V34.1.242), Parasolid V35.0 (All versions < V35.0.161), Parasolid V35.0 (All versions >= V35.0.161 < V35.0.164), Simcenter Femap V2022.1 (All versions < V2022.1.3), Simcenter Femap V2022.2 (All versions < V2022.2.2). The affected application contains an out of bounds write past the end of an allocated buffer while parsing specially crafted X_T files. This could allow an attacker to execute code in the context of the current process. (ZDI-CAN-17740)	7.8	More Details
CVE-2022-39151	A vulnerability has been identified in Parasolid V33.1 (All versions < V33.1.262), Parasolid V33.1 (All versions >= V33.1.262 < V33.1.263), Parasolid V34.0 (All versions < V34.0.252), Parasolid V34.1 (All versions < V34.1.242), Parasolid V35.0 (All versions < V35.0.161), Parasolid V35.0 (All versions >= V35.0.161 < V35.0.164), Simcenter Femap V2022.1 (All versions < V2022.1.3), Simcenter Femap V2022.2 (All versions < V2022.2.2). The affected application contains an out of bounds write past the end of an allocated buffer while parsing specially crafted X_T files. This could allow an attacker to execute code in the context of the current process. (ZDI-CAN-17736)	7.8	More Details
CVE-2022-39150	A vulnerability has been identified in Parasolid V33.1 (All versions < V33.1.262), Parasolid V33.1 (All versions >= V33.1.262 < V33.1.263), Parasolid V34.0 (All versions < V34.0.252), Parasolid V34.1 (All versions < V34.1.242), Parasolid V35.0 (All versions < V35.0.161), Parasolid V35.0 (All versions >= V35.0.161 < V35.0.164), Simcenter Femap V2022.1 (All versions < V2022.1.3), Simcenter Femap V2022.2 (All versions < V2022.2.2). The affected application contains an out of bounds write past the end of an allocated buffer while parsing specially crafted X_T files. This could allow an attacker to execute code in the context of the current process. (ZDI-CAN-17735)	7.8	More Details
CVE-2022-38005	Windows Print Spooler Elevation of Privilege Vulnerability	7.8	More Details
CVE-2022-35292	In SAP Business One application when a service is created, the executable path contains spaces and isn't enclosed within quotes, leading to a vulnerability known as Unquoted Service Path which allows a user to gain SYSTEM privileges. If the service is exploited by adversaries, it can be used to gain privileged permissions on a system or network leading to high impact on Confidentiality, Integrity, and Availability.	7.8	More Details
CVE-2022-39119	In network service, there is a missing permission check. This could lead to local escalation of privilege with no additional execution privileges needed	7.8	More Details
CVE-2022-37957	Windows Kernel Elevation of Privilege Vulnerability	7.8	More Details
CVE-2022-39155	A vulnerability has been identified in Parasolid V33.1 (All versions < V33.1.262), Parasolid V33.1 (All versions >= V33.1.262 < V33.1.263), Parasolid V34.0 (All versions < V34.0.252), Parasolid V34.1 (All versions < V34.1.242), Parasolid V35.0 (All versions < V35.0.161), Parasolid V35.0 (All versions >= V35.0.161 < V35.0.164), Simcenter Femap V2022.1 (All versions < V2022.1.3), Simcenter Femap V2022.2 (All versions < V2022.2.2). The affected application contains an out of bounds write past the end of an allocated buffer while parsing specially crafted X_T files. This could allow an attacker to execute code in the context of the current process. (ZDI-CAN-18192)	7.8	More Details

CVE Number	Description	Base Score	Reference
CVE-2022-38466	A vulnerability has been identified in CoreShield One-Way Gateway (OWG) Software (All versions < V2.2). The default installation sets insecure file permissions that could allow a local attacker to escalate privileges to local administrator.	7.8	More Details
CVE-2022-38007	Azure Guest Configuration and Azure Arc-enabled servers Elevation of Privilege Vulnerability	7.8	More Details
CVE-2022-39149	A vulnerability has been identified in Parasolid V33.1 (All versions < V33.1.262), Parasolid V33.1 (All versions >= V33.1.262 < V33.1.263), Parasolid V34.0 (All versions < V34.0.252), Parasolid V34.1 (All versions < V34.1.242), Parasolid V35.0 (All versions < V35.0.161), Parasolid V35.0 (All versions >= V35.0.161 < V35.0.164), Simcenter Femap V2022.1 (All versions < V2022.1.3), Simcenter Femap V2022.2 (All versions < V2022.2.2). The affected application contains an out of bounds write past the end of an allocated buffer while parsing specially crafted X_T files. This could allow an attacker to execute code in the context of the current process. (ZDI-CAN-17733)	7.8	More Details
CVE-2022-39147	A vulnerability has been identified in Parasolid V33.1 (All versions < V33.1.262), Parasolid V33.1 (All versions >= V33.1.262 < V33.1.263), Parasolid V34.0 (All versions < V34.0.252), Parasolid V34.1 (All versions < V34.1.242), Parasolid V35.0 (All versions < V35.0.161), Parasolid V35.0 (All versions >= V35.0.161 < V35.0.164), Simcenter Femap V2022.1 (All versions < V2022.1.3), Simcenter Femap V2022.2 (All versions < V2022.2.2). The affected application is vulnerable to uninitialized pointer access while parsing specially crafted X_T files. An attacker could leverage this vulnerability to execute code in the context of the current process. (ZDI-CAN-17506)	7.8	More Details
CVE-2022-40297	UBports Ubuntu Touch 16.04 allows the screen-unlock passcode to be used for a privileged shell via Sudo. This passcode is only four digits, far below typical length/complexity for a user account's password. NOTE: a third party states "The described attack cannot be executed as demonstrated.	7.8	More Details
CVE-2022-35828	Microsoft Defender for Endpoint for Mac Elevation of Privilege Vulnerability	7.8	More Details
CVE-2022-40299	In Singular before 4.3.1, a predictable /tmp pathname is used (e.g., by sdb.cc), which allows local users to gain the privileges of other users via a procedure in a file under /tmp. NOTE: this CVE Record is about sdb.cc and similar files in the Singular interface that have predictable /tmp pathnames; this CVE Record is not about the lack of a safe temporary-file creation capability in the Singular language.	7.8	More Details
CVE-2022-31322	Penta Security Systems Inc WAPPLES v6.0 r3 4.10-hotfix1 allows attackers to escalate privileges via overwriting files using SUID flagged executables.	7.8	More Details
CVE-2022-36403	Untrusted search path vulnerability in the installer of Device Software Manager prior to Ver.2.20.3.0 allows an attacker to gain privileges via a Trojan horse DLL in an unspecified directory.	7.8	More Details
CVE-2022-38633	Genymotion Desktop v3.2.1 was discovered to contain a DLL hijacking vulnerability which allows attackers to escalate privileges and execute arbitrary code via a crafted binary.	7.8	More Details
CVE-2022-34101	A vulnerability was discovered in the Crestron AirMedia Windows Application, version 4.3.1.39, in which a user can place a malicious DLL in a certain path to execute code and preform a privilege escalation attack.	7.8	More Details
CVE-2022-35803	Windows Common Log File System Driver Elevation of Privilege Vulnerability	7.8	More Details
CVE-2022-34729	Windows GDI Elevation of Privilege Vulnerability	7.8	More Details
CVE-2022-36271	Outbyte PC Repair Installation File 1.7.112.7856 is vulnerable to Dll Hijacking. iertutil.dll is missing so an attacker can use a malicious dll with same name and can get admin privileges.	7.8	More Details

CVE Number	Description	Base Score	Reference
CVE-2022-34719	Windows Distributed File System (DFS) Elevation of Privilege Vulnerability	7.8	More Details
CVE-2022-2964	A flaw was found in the Linux kernel's driver for the ASIX AX88179_178A-based USB 2.0/3.0 Gigabit Ethernet Devices. The vulnerability contains multiple out-of-bounds reads and possible out-of-bounds writes.	7.8	More Details
CVE-2022-36049	Flux2 is a tool for keeping Kubernetes clusters in sync with sources of configuration, and Flux's helm-controller is a Kubernetes operator that allows one to declaratively manage Helm chart releases. Helm controller is tightly integrated with the Helm SDK. A vulnerability found in the Helm SDK that affects flux2 v0.0.17 until v0.32.0 and helm-controller v0.0.4 until v0.23.0 allows for specific data inputs to cause high memory consumption. In some platforms, this could cause the controller to panic and stop processing reconciliations. In a shared cluster multi-tenancy environment, a tenant could create a HelmRelease that makes the controller panic, denying all other tenants from their Helm releases being reconciled. Patches are available in flux2 v0.32.0 and helm-controller v0.23.0.	7.7	More Details
CVE-2022-38012	Microsoft Edge (Chromium-based) Remote Code Execution Vulnerability	7.7	More Details
CVE-2022-36091	XWiki Platform Web Templates are templates for XWiki Platform, a generic wiki platform. Through the suggestion feature, string and list properties of objects the user shouldn't have access to can be accessed in versions prior to 13.10.4 and 14.2. This includes private personal information like email addresses and salted password hashes of registered users but also other information stored in properties of objects. Sensitive configuration fields like passwords for LDAP or SMTP servers could be accessed. By exploiting an additional vulnerability, this issue can even be exploited on private wikis at least for string properties. The issue is patched in version 13.10.4 and 14.2. Password properties are no longer displayed and rights are checked for other properties. A workaround is available. The template file `suggest.vm` can be replaced by a patched version without upgrading or restarting XWiki unless it has been overridden, in which case the overridden template should be patched, too. This might need adjustments for older versions, though.	7.5	More Details
CVE-2022-3174	Sensitive Cookie in HTTPS Session Without 'Secure' Attribute in GitHub repository ikus060/rdiffweb prior to 2.4.2.	7.5	More Details
CVE-2022-1278	A flaw was found in WildFly, where an attacker can see deployment names, endpoints, and any other data the trace payload may contain.	7.5	More Details
CVE-2021-37819	PDF Labs pdftk-java v3.2.3 was discovered to contain an infinite loop via the component /text/pdf/PdfReader.java.	7.5	More Details
CVE-2022-34724	Windows DNS Server Denial of Service Vulnerability	7.5	More Details
CVE-2022-31006	indy-node is the server portion of Hyperledger Indy, a distributed ledger purpose-built for decentralized identity. In vulnerable versions of indy-node, an attacker can max out the number of client connections allowed by the ledger, leaving the ledger unable to be used for its intended purpose. However, the ledger content will not be impacted and the ledger will resume functioning after the attack. This attack exploits the trade-off between resilience and availability. Any protection against abusive client connections will also prevent the network being accessed by certain legitimate users. As a result, validator nodes must tune their firewall rules to ensure the right trade-off for their network's expected users. The guidance to network operators for the use of firewall rules in the deployment of Indy networks has been modified to better protect against denial of service attacks by increasing the cost and complexity in mounting such attacks. The mitigation for this vulnerability is not in the Hyperledger Indy code per se, but rather in the individual deployments of Indy. The mitigations should be applied to all deployments of Indy, and are not related to a particular release.	7.5	More Details
CVE-2022-35838	HTTP V3 Denial of Service Vulnerability	7.5	More Details

CVE Number	Description	Base Score	Reference
CVE-2022-40281	An issue was discovered in Samsung TizenRT through 3.0_GBM (and 3.1_PRE). cyassl_connect_step2 in curl/vtls/cyassl.c has a missing X509_free after SSL_get_peer_certificate, leading to information disclosure.	7.5	More Details
CVE-2022-28740	aEnrich eHRD Learning Management Key Performance Indicator System 5+ exposes Sensitive Information to an Unauthorized Actor.	7.5	More Details
CVE-2022-36092	XWiki Platform Old Core is a core package for XWiki Platform, a generic wiki platform. Prior to versions 14.2 and 13.10.4, all rights checks that would normally prevent a user from viewing a document on a wiki can be bypassed using the login action and directly specified templates. This exposes title, content and comments of any document and properties of objects, though class and property name must be known. This is also exploitable on private wikis. This has been patched in versions 14.2 and 13.10.4 by properly checking view rights before loading documents and disallowing non-default templates in the login, registration and skin action. As a workaround, it would be possible to protect all templates individually by adding code to check access rights first.	7.5	More Details
CVE-2022-38100	The CMS800 device fails while attempting to parse malformed network data sent by a threat actor. A threat actor with network access can remotely issue a specially formatted UDP request that will cause the entire device to crash and require a physical reboot. A UDP broadcast request could be sent that causes a mass denial-of-service attack on all CME8000 devices connected to the same network.	7.5	More Details
CVE-2022-40280	An issue was discovered in Samsung TizenRT through 3.0_GBM (and 3.1_PRE). createDB in security/provisioning/src/provisioningdatabasemanager.c has a missing sqlite3_close after sqlite3_open_v2, leading to a denial of service.	7.5	More Details
CVE-2022-28742	aEnrich eHRD Learning Management Key Performance Indicator System 5+ has Improper Access Control. The web application does not validate user session when accessing many application pages. This can allow an attacker to gain unauthenticated access to sensitive functionalities in the application	7.5	More Details
CVE-2022-34720	Windows Internet Key Exchange (IKE) Extension Denial of Service Vulnerability	7.5	More Details
CVE-2022-37857	bilde2910 Hauk v1.6.1 requires a hardcoded password which by default is blank. This hardcoded password is hashed but stored within the config.php file server-side as well as in clear-text on the android client device by default.	7.5	More Details
CVE-2022-38614	An issue in the IGB Files and OutfileService features of SmartVista Cardgen v3.28.0 allows attackers to list and download arbitrary files via modifying the PATH parameter.	7.5	More Details
CVE-2022-20696	A vulnerability in the binding configuration of Cisco SD-WAN vManage Software containers could allow an unauthenticated, adjacent attacker who has access to the VPN0 logical network to also access the messaging service ports on an affected system. This vulnerability exists because the messaging server container ports on an affected system lack sufficient protection mechanisms. An attacker could exploit this vulnerability by connecting to the messaging service ports of the affected system. To exploit this vulnerability, the attacker must be able to send network traffic to interfaces within the VPN0 logical network. This network may be restricted to protect logical or physical adjacent networks, depending on device deployment configuration. A successful exploit could allow the attacker to view and inject messages into the messaging service, which can cause configuration changes or cause the system to reload.	7.5	More Details
CVE-2022-36255	A SQL injection vulnerability in SupplierDAO.java in sazanrjb InventoryManagementSystem 1.0 allows attackers to execute arbitrary SQL commands via the parameters such as "searchTxt".	7.5	More Details
CVE-2022-37189	DDMAL MEI2Volpiano 0.8.2 is vulnerable to XML External Entity (XXE), leading to a Denial of Service. This occurs due to the usage of the unsafe 'xml.etree' library to parse untrusted XML input.	7.5	More Details
CVE-2022-40023	Sqlalchemy mako before 1.2.2 is vulnerable to Regular expression Denial of Service when using the Lexer class to parse. This also affects babelplugin and linguaplugin.	7.5	More Details

CVE Number	Description	Base Score	Reference
CVE-2022-35513	The Blink1Control2 application <= 2.2.7 uses weak password encryption and an insecure method of storage.	7.5	More Details
CVE-2022-31414	D-Link DIR-1960 firmware DIR-1960_A1_1.11 was discovered to contain a buffer overflow via srtcat in prog.cgi. This vulnerability allowed attackers to cause a Denial of Service (DoS) via a crafted HTTP request.	7.5	More Details
CVE-2022-36539	WeDayCare B.V Ouderapp before v1.1.22 allows attackers to alter the ID value within intercepted calls to gain access to data of other parents and children.	7.5	More Details
CVE-2022-35572	On Linksys E5350 WiFi Router with firmware version 1.0.00.037 and lower, (and potentially other vendors/devices due to code reuse), the /SysInfo.htm URI does not require a session ID. This web page calls a show_sysinfo function which retrieves WPA passwords, SSIDs, MAC Addresses, serial numbers, WPS Pins, and hardware/firmware versions, and prints this information into the web page. This web page is visible when remote management is enabled. A user who has access to the web interface of the device can extract these secrets. If the device has remote management enabled and is connected directly to the internet, this vulnerability is exploitable over the internet without interaction.	7.5	More Details
CVE-2022-36081	Wikmd is a file based wiki that uses markdown. Prior to version 1.7.1, Wikmd is vulnerable to path traversal when accessing `/list/<path:folderpath>` and discloses lists of files located on the server including sensitive data. Version 1.7.1 fixes this issue.	7.5	More Details
CVE-2022-38769	The mobile application in Transtek Mojodat FAM (Fixed Asset Management) 2.4.6 allows remote attackers to fetch cleartext passwords upon a successful login request.	7.5	More Details
CVE-2022-37145	The PlexTrac platform prior to version 1.17.0 does not restrict excessive authentication attempts for accounts configured to use the PlexTrac authentication provider. An unauthenticated remote attacker could perform a bruteforce attack on the login page with no time or attempt limitation in an attempt to obtain valid credentials for the platform users configured to use the PlexTrac authentication provider.	7.5	More Details
CVE-2022-28220	Apache James prior to release 3.6.3 and 3.7.1 is vulnerable to a buffering attack relying on the use of the STARTTLS command. Fix of CVE-2021-38542, which solved similar problem fron Apache James 3.6.1, is subject to a parser differential and do not take into account concurrent requests.	7.5	More Details
CVE-2022-1700	Improper Restriction of XML External Entity Reference ('XXE') vulnerability in the Policy Engine of Forcepoint Data Loss Prevention (DLP), which is also leveraged by Forcepoint One Endpoint (F1E), Web Security Content Gateway, Email Security with DLP enabled, and Cloud Security Gateway prior to June 20, 2022. The XML parser in the Policy Engine was found to be improperly configured to support external entities and external DTD (Document Type Definitions), which can lead to an XXE attack. This issue affects: Forcepoint Data Loss Prevention (DLP) versions prior to 8.8.2. Forcepoint One Endpoint (F1E) with Policy Engine versions prior to 8.8.2. Forcepoint Web Security Content Gateway versions prior to 8.5.5. Forcepoint Email Security with DLP enabled versions prior to 8.5.5. Forcepoint Cloud Security Gateway prior to June 20, 2022.	7.5	More Details
CVE-2022-37797	In lighttpd 1.4.65, mod_wstunnel does not initialize a handler function pointer if an invalid HTTP request (websocket handshake) is received. It leads to null pointer dereference which crashes the server. It could be used by an external attacker to cause denial of service condition.	7.5	More Details
CVE-2022-37734	graphql-java before19.0 is vulnerable to Denial of Service. An attacker can send a malicious GraphQL query that consumes CPU resources. The fixed versions are 19.0 and later, 18.3, and 17.4, and 0.0.0-2022-07-26T05-45-04-226aabd9.	7.5	More Details
CVE-2022-37835	Torguard VPN 4.8, has a vulnerability that allows an attacker to dump sensitive information, such as credentials and information about the server, without admin privileges.	7.5	More Details
CVE-2022-36259	A SQL injection vulnerability in ConnectionFactory.java in sazanrjb InventoryManagementSystem 1.0 allows attackers to execute arbitrary SQL commands via the parameters such as "username", "password", etc.	7.5	More Details
CVE-2022-36258	A SQL injection vulnerability in CustomerDAO.java in sazanrjb InventoryManagementSystem 1.0 allows attackers to execute arbitrary SQL commands via the parameters such as "searchTxt".	7.5	More Details

CVE Number	Description	Base Score	Reference
CVE-2022-36256	A SQL injection vulnerability in Stocks.java in sazanrjb InventoryManagementSystem 1.0 allows attackers to execute arbitrary SQL commands via the parameters such as "productcode".	7.5	More Details
CVE-2022-36257	A SQL injection vulnerability in UserDAO.java in sazanrjb InventoryManagementSystem 1.0 allows attackers to execute arbitrary SQL commands via the parameters such as "users", "pass", etc.	7.5	More Details
CVE-2022-35833	Windows Secure Channel Denial of Service Vulnerability	7.5	More Details
CVE-2022-39801	SAP GRC Access control Emergency Access Management allows an authenticated attacker to access a Firefighter session even after it is closed in Firefighter Logon Pad. This attack can be launched only within the firewall. On successful exploitation the attacker can gain access to admin session and completely compromise the application.	7.5	More Details
CVE-2022-38013	.NET Core and Visual Studio Denial of Service Vulnerability	7.5	More Details
CVE-2022-3029	In NLnet Labs Routinator 0.9.0 up to and including 0.11.2, due to a mistake in error handling, data in RRDP snapshot and delta files that isn't correctly base 64 encoded is treated as a fatal error and causes Routinator to exit. Worst case impact of this vulnerability is denial of service for the RPKI data that Routinator provides to routers. This may stop your network from validating route origins based on RPKI data. This vulnerability does not allow an attacker to manipulate RPKI data.	7.5	More Details
CVE-2022-39208	Onedev is an open source, self-hosted Git Server with CI/CD and Kanban. All files in the /opt/onedev/sites/ directory are exposed and can be read by unauthenticated users. This directory contains all projects, including their bare git repos and build artifacts. This file disclosure vulnerability can be used by unauthenticated attackers to leak all project files of any project. Since project IDs are incremental, an attacker could iterate through them and leak all project data. This issue has been resolved in version 7.3.0 and users are advised to upgrade. There are no known workarounds for this issue.	7.5	More Details
CVE-2022-39821	In NOKIA 1350 OMS R14.2, an Insertion of Sensitive Information into an Application Log File vulnerability occurs. The web application stores critical information, such as cleartext user credentials, in world-readable files in the filesystem.	7.5	More Details
CVE-2022-40621	Because the WAVLINK Quantum D4G (WN531G3) running firmware version M31G3.V5030.200325 and earlier communicates over HTTP and not HTTPS, and because the hashing mechanism does not rely on a server-supplied key, it is possible for an attacker with sufficient network access to capture the hashed password of a logged on user and use it in a classic Pass-the-Hash style attack.	7.5	More Details
CVE-2020-10735	A flaw was found in python. In algorithms with quadratic time complexity using non-binary bases, when using int("text"), a system could take 50ms to parse an int string with 100,000 digits and 5s for 1,000,000 digits (float, decimal, int.from_bytes(), and int() for binary bases 2, 4, 8, 16, and 32 are not affected). The highest threat from this vulnerability is to system availability.	7.5	More Details
CVE-2022-32190	JoinPath and URL.JoinPath do not remove ../ path elements appended to a relative path. For example, JoinPath("https://go.dev", "../go") returns the URL "https://go.dev/../go", despite the JoinPath documentation stating that ../ path elements are removed from the result.	7.5	More Details
CVE-2022-36423	OpenHarmony-v3.1.2 and prior versions have an incorrect configuration of the cJSON library, which leads a Stack overflow vulnerability during recursive parsing. LAN attackers can lead a DoS attack to all network devices.	7.4	More Details
CVE-2022-36085	Open Policy Agent (OPA) is an open source, general-purpose policy engine. The Rego compiler provides a (deprecated) `WithUnsafeBuiltins` function, which allows users to provide a set of built-in functions that should be deemed unsafe — and as such rejected — by the compiler if encountered in the policy compilation stage. A bypass of this protection has been found, where the use of the `with` keyword to mock such a built-in function (a feature introduced in OPA v0.40.0), isn't taken into account by `WithUnsafeBuiltins`. Multiple conditions need to be met in order to create an adverse effect. Version 0.43.1 contains a patch for this issue. As a workaround, avoid using the `WithUnsafeBuiltins` function and use the `capabilities` feature instead.	7.4	More Details

CVE Number	Description	Base Score	Reference
CVE-2022-3130	A vulnerability classified as critical has been found in codeprojects Online Driving School. This affects an unknown part of the file /login.php. The manipulation of the argument username leads to sql injection. It is possible to initiate the attack remotely. The exploit has been disclosed to the public and may be used. The identifier VDB-207873 was assigned to this vulnerability.	7.3	More Details
CVE-2022-38020	Visual Studio Code Elevation of Privilege Vulnerability	7.3	More Details
CVE-2022-36070	Poetry is a dependency manager for Python. To handle dependencies that come from a Git repository, Poetry executes various commands, e.g. `git config`. These commands are being executed using the executable's name and not its absolute path. This can lead to the execution of untrusted code due to the way Windows resolves executable names to paths. Unlike Linux-based operating systems, Windows searches for the executable in the current directory first and looks in the paths that are defined in the `PATH` environment variable afterward. This vulnerability can lead to Arbitrary Code Execution, which would lead to the takeover of the system. If a developer is exploited, the attacker could steal credentials or persist their access. If the exploit happens on a server, the attackers could use their access to attack other internal systems. Since this vulnerability requires a fair amount of user interaction, it is not as dangerous as a remotely exploitable one. However, it still puts developers at risk when dealing with untrusted files in a way they think is safe. The victim could also not protect themself by vetting any Git or Poetry config files that might be present in the directory, because the behavior is undocumented. Versions 1.1.9 and 1.2.0b1 contain patches for this issue.	7.3	More Details
CVE-2022-36069	Poetry is a dependency manager for Python. When handling dependencies that come from a Git repository instead of a registry, Poetry uses various commands, such as `git clone`. These commands are constructed using user input (e.g. the repository URL). When building the commands, Poetry correctly avoids Command Injection vulnerabilities by passing an array of arguments instead of a command string. However, there is the possibility that a user input starts with a dash (`-`) and is therefore treated as an optional argument instead of a positional one. This can lead to Code Execution because some of the commands have options that can be leveraged to run arbitrary executables. If a developer is exploited, the attacker could steal credentials or persist their access. If the exploit happens on a server, the attackers could use their access to attack other internal systems. Since this vulnerability requires a fair amount of user interaction, it is not as dangerous as a remotely exploitable one. However, it still puts developers at risk when dealing with untrusted files in a way they think is safe, because the exploit still works when the victim tries to make sure nothing can happen, e.g. by vetting any Git or Poetry config files that might be present in the directory. Versions 1.1.9 and 1.2.0b1 contain patches for this issue.	7.3	More Details
CVE-2022-39200	Dendrite is a Matrix homeserver written in Go. In affected versions events retrieved from a remote homeserver using the `/get_missing_events` path did not have their signatures verified correctly. This could potentially allow a remote homeserver to provide invalid/modified events to Dendrite via this endpoint. Note that this does not apply to events retrieved through other endpoints (e.g. `/event`, `/state`) as they have been correctly verified. Homeservers that have federation disabled are not vulnerable. The problem has been fixed in Dendrite 0.9.8. Users are advised to upgrade. There are no known workarounds for this issue.	7.3	More Details
CVE-2022-38011	Raw Image Extension Remote Code Execution Vulnerability	7.3	More Details
CVE-2022-30170	Windows Credential Roaming Service Elevation of Privilege Vulnerability	7.3	More Details
CVE-2022-25765	The package pdfkit from 0.0.0 are vulnerable to Command Injection where the URL is not properly sanitized.	7.3	More Details
CVE-2022-38279	JFinal CMS 5.1.0 is vulnerable to SQL Injection via /admin/imagealbum/list.	7.2	More Details
CVE-2022-38273	JFinal CMS 5.1.0 is vulnerable to SQL Injection via /admin/article/list_approve.	7.2	More Details

CVE Number	Description	Base Score	Reference
CVE-2022-38276	JFinal CMS 5.1.0 is vulnerable to SQL Injection via /admin/foldernotice/list.	7.2	More Details
CVE-2022-38283	JFinal CMS 5.1.0 is vulnerable to SQL Injection via /admin/video/list.	7.2	More Details
CVE-2022-38272	JFinal CMS 5.1.0 is vulnerable to SQL Injection via /admin/article/list.	7.2	More Details
CVE-2022-37777	Phicomm FIR151B A2, FIR302E A2, FIR300B A2, FIR303B A2 routers 3.0.1.17 and earlier were discovered to contain a remote command execution (RCE) vulnerability via the trHops parameter of the tracert function.	7.2	More Details
CVE-2022-38277	JFinal CMS 5.1.0 is vulnerable to SQL Injection via /admin/folderrollpicture/list.	7.2	More Details
CVE-2022-38284	JFinal CMS 5.1.0 is vulnerable to SQL Injection via /system/department/list.	7.2	More Details
CVE-2022-37778	Phicomm FIR151B A2, FIR302E A2, FIR300B A2, FIR303B A2 routers V3.0.1.17 were discovered to contain a remote command execution (RCE) vulnerability via the current_time parameter of the time function.	7.2	More Details
CVE-2022-37779	Phicomm FIR151B A2, FIR302E A2, FIR300B A2, FIR303B A2 routers V3.0.1.17 were discovered to contain a remote command execution (RCE) vulnerability via the sendnum parameter of the ping function.	7.2	More Details
CVE-2022-38282	JFinal CMS 5.1.0 is vulnerable to SQL Injection via /admin/videoalbum/list.	7.2	More Details
CVE-2022-38278	JFinal CMS 5.1.0 is vulnerable to SQL Injection via /admin/friendlylink/list.	7.2	More Details
CVE-2022-38281	JFinal CMS 5.1.0 is vulnerable to SQL Injection via /admin/site/list.	7.2	More Details
CVE-2022-36103	Talos Linux is a Linux distribution built for Kubernetes deployments. Talos worker nodes use a join token to get accepted into the Talos cluster. Due to improper validation of the request while signing a worker node CSR (certificate signing request) Talos control plane node might issue Talos API certificate which allows full access to Talos API on a control plane node. Accessing Talos API with full level access on a control plane node might reveal sensitive information which allows full level access to the cluster (Kubernetes and Talos PKI, etc.). Talos API join token is stored in the machine configuration on the worker node. When configured correctly, Kubernetes workloads don't have access to the machine configuration, but due to a misconfiguration workload might access the machine configuration and reveal the join token. This problem has been fixed in Talos 1.2.2. Enabling the Pod Security Standards mitigates the vulnerability by denying hostPath mounts and host networking by default in the baseline policy. Clusters that don't run untrusted workloads are not affected. Clusters with correct Pod Security configurations which don't allow hostPath mounts, and secure access to cloud metadata server (or machine configuration is not supplied via cloud metadata server) are not affected.	7.2	More Details
CVE-2022-38280	JFinal CMS 5.1.0 is vulnerable to SQL Injection via /admin/image/list.	7.2	More Details
CVE-2022-38605	Church Management System v1.0 was discovered to contain a SQL injection vulnerability via the id parameter at /admin/edit_event.php.	7.2	More Details

CVE Number	Description	Base Score	Reference
CVE-2022-38285	JFinal CMS 5.1.0 is vulnerable to SQL Injection via /system/menu/list.	7.2	More Details
CVE-2022-38255	Interview Management System v1.0 was discovered to contain a SQL injection vulnerability via the id parameter at /interview/editQuestion.php.	7.2	More Details
CVE-2022-37780	Phicomm FIR151B A2, FIR302E A2, FIR300B A2, FIR303B A2 routers V3.0.1.17 were discovered to contain a remote command execution (RCE) vulnerability via the pingAddr parameter of the tracert function.	7.2	More Details
CVE-2022-29061	An improper neutralization of special elements used in an OS command ('OS Command Injection') vulnerability [CWE-78] in Fortinet FortiSOAR before 7.2.1 allows an authenticated attacker to execute unauthorized code or commands via crafted HTTP GET requests.	7.2	More Details
CVE-2022-1807	Multiple SQLi vulnerabilities in Webadmin allow for privilege escalation from admin to super-admin in Sophos Firewall older than version 18.5 MR4 and version 19.0 MR1.	7.2	More Details
CVE-2022-38304	Online Leave Management System v1.0 was discovered to contain a SQL injection vulnerability via the id parameter at /maintenance/manage_leave_type.php.	7.2	More Details
CVE-2022-38269	School Activity Updates with SMS Notification v1.0 was discovered to contain a SQL injection vulnerability via the component /modules/modstudent/index.php?view=edit&id=.	7.2	More Details
CVE-2022-38303	Online Leave Management System v1.0 was discovered to contain a SQL injection vulnerability via the id parameter at /employees/manage_leave_type.php.	7.2	More Details
CVE-2022-38302	Online Leave Management System v1.0 was discovered to contain a SQL injection vulnerability via the id parameter at /maintenance/manage_department.php.	7.2	More Details
CVE-2022-38268	School Activity Updates with SMS Notification v1.0 was discovered to contain a SQL injection vulnerability via the component /modules/autonumber/index.php?view=edit&id=.	7.2	More Details
CVE-2022-38267	School Activity Updates with SMS Notification v1.0 was discovered to contain a SQL injection vulnerability via the component /modules/user/index.php?view=edit&id=.	7.2	More Details
CVE-2022-38265	Apartment Visitor Management System v1.0 was discovered to contain a SQL injection vulnerability via the editid parameter at /avms/edit-apartment.php.	7.2	More Details
CVE-2022-38286	JFinal CMS 5.1.0 is vulnerable to SQL Injection via /system/role/list.	7.2	More Details
CVE-2022-38610	Garage Management System v1.0 was discovered to contain a SQL injection vulnerability via the id parameter at /garage/editclient.php.	7.2	More Details
CVE-2022-38606	Garage Management System v1.0 was discovered to contain a SQL injection vulnerability via the id parameter at /garage/editcategory.php.	7.2	More Details
CVE-2022-38274	JFinal CMS 5.1.0 is vulnerable to SQL Injection via /admin/comment/list.	7.2	More Details

CVE Number	Description	Base Score	Reference
CVE-2022-38260	Interview Management System v1.0 was discovered to contain a SQL injection vulnerability via the component /interview/delete.php?action=questiondelete&id=.	7.2	More Details
CVE-2022-38275	JFinal CMS 5.1.0 is vulnerable to SQL Injection via /admin/contact/list.	7.2	More Details
CVE-2022-31226	Dell BIOS versions contain a Stack-based Buffer Overflow vulnerability. A local authenticated malicious user could potentially exploit this vulnerability by sending excess data to a function in order to gain arbitrary code execution on the system.	7.1	More Details
CVE-2022-31167	XWiki Platform Security Parent POM contains the security APIs for XWiki Platform, a generic wiki platform. Starting with version 5.0 and prior to 12.10.11, 13.10.1, and 13.4.6, a bug in the security cache stores rules associated to document Page1.Page2 and space Page1.Page2 in the same cache entry. That means that it's possible to overwrite the rights of a space or a document by creating the page of the space with the same name and checking the right of the new one first so that they end up in the security cache and are used for the other too. The problem has been patched in XWiki 12.10.11, 13.10.1, and 13.4.6. There are no known workarounds.	7.1	More Details
CVE-2022-34109	An issue in Micro-Star International MSI Feature Navigator v1.0.1808.0901 allows attackers to write arbitrary files to the directory \PromoPhoto\, regardless of file type or size.	7.1	More Details
CVE-2022-34108	An issue in the Feature Navigator of Micro-Star International MSI Feature Nagivator v1.0.1808.0901 allows attackers to cause a Denial of Service (DoS) via a crafted image or video file.	7.1	More Details
CVE-2022-2990	An incorrect handling of the supplementary groups in the Buildah container engine might lead to the sensitive information disclosure or possible data modification if an attacker has direct access to the affected container where supplementary groups are used to set access permissions and is able to execute a binary code in that container.	7.1	More Details
CVE-2022-2989	An incorrect handling of the supplementary groups in the Podman container engine might lead to the sensitive information disclosure or possible data modification if an attacker has direct access to the affected container where supplementary groups are used to set access permissions and is able to execute a binary code in that container.	7.1	More Details
CVE-2022-3182	Improper Access Control vulnerability in the Duo SMS two-factor of Devolutions Remote Desktop Manager 2022.2.14 and earlier allows attackers to bypass the application lock. This issue affects: Devolutions Remote Desktop Manager version 2022.2.14 and prior versions.	7.0	More Details
CVE-2022-34725	Windows ALPC Elevation of Privilege Vulnerability	7.0	More Details
CVE-2022-26928	Windows Photo Import API Elevation of Privilege Vulnerability	7.0	More Details
CVE-2021-0697	In PVRSRVRGXSubmitTransferKM of rgxtransfer.c, there is a possible user after free due to a race condition. This could lead to local escalation of privilege with no additional execution privileges needed. User interaction is not needed for exploitation.Product: AndroidVersions: Android SoCAndroid ID: A-238918403	7.0	More Details
CVE-2022-38399	Missing protection mechanism for alternate hardware interface in SmaCam CS-QR10 all versions and SmaCam Night Vision CS-QR20 all versions allows an attacker to execute an arbitrary OS command by having the product connect to the product's specific serial connection	6.8	More Details
CVE-2022-36385	A threat actor with momentary access to the device can plug in a USB drive and perform a malicious firmware update, resulting in permanent changes to device functionality. No authentication or controls are in place to prevent a threat actor from maliciously modifying firmware and performing a drive-by attack to load the firmware on any CMS8000 device.	6.8	More Details
CVE-2022-36376	Server-Side Request Forgery (SSRF) vulnerability in Rank Math SEO plugin <= 1.0.95 at WordPress.	6.8	More Details

CVE Number	Description	Base Score	Reference
CVE-2022-36869	Improper access control vulnerability in ContactsDumpActivity of?Contacts Provider prior to version 12.7.59 allows attacker to access the file without permission.	6.6	More Details
CVE-2022-36875	Improper restriction of broadcasting Intent in SaWebViewRelayActivity of?Waterplugin prior to version 2.2.11.22081151 allows attacker to access the file without permission.	6.6	More Details
CVE-2022-37299	An issue was discovered in Shirne CMS 1.2.0. There is a Path Traversal vulnerability which could cause arbitrary file read via /static/ueditor/php/controller.php	6.5	More Details
CVE-2022-36779	PROSCEND - PROSCEND / ADVICE .Ltd - G/5G Industrial Cellular Router (with GPS)4 Unauthenticated OS Command Injection Proscend M330-w / M33-W5 / M350-5G / M350-W5G / M350-6 / M350-W6 / M301-G / M301-GW ADVICE ICR 111WG / https://www.proscend.com/en/category/industrial-Cellular-Router/industrial-Cellular-Router.html https://cdn.shopify.com/s/files/1/0036/9413/3297/files/ADVICE_Industrial_4G_LTE_Cellular_Router_ICR111WG.pdf?v=1620814301	6.5	More Details
CVE-2022-39816	In NOKIA 1350 OMS R14.2, Insufficiently Protected Credentials (cleartext administrator password) occur in the edit configuration page. Exploitation requires an authenticated attacker.	6.5	More Details
CVE-2022-38613	A Path Traversal vulnerability in SmartVista Cardgen v3.28.0 allows authenticated attackers to read arbitrary files in the system.	6.5	More Details
CVE-2022-2528	In affected versions of Octopus Deploy it is possible to upload a package to built-in feed with insufficient permissions after re-indexing packages.	6.5	More Details
CVE-2022-36793	Unauthenticated Plugin Settings Change & Data Deletion vulnerabilities in WP Shop plugin <= 3.9.6 at WordPress.	6.5	More Details
CVE-2022-38067	Unauthenticated Event Deletion vulnerability in Totalsoft Event Calendar – Calendar plugin <= 1.4.6 at WordPress.	6.5	More Details
CVE-2022-36661	xhyve commit dfbe09b was discovered to contain a NULL pointer dereference via the component vi_pci_read(). This vulnerability allows attackers to cause a Denial of Service via unspecified vectors.	6.5	More Details
CVE-2022-36778	insert HTML / js code inside input how to get to the vulnerable input : Workers > worker nickname > inject in this input the code.	6.5	More Details
CVE-2022-36659	xhyve commit dfbe09b was discovered to contain a NULL pointer dereference via the component vi_pci_write(). This vulnerability allows attackers to cause a Denial of Service via unspecified vectors.	6.5	More Details
CVE-2022-35837	Windows Graphics Component Information Disclosure Vulnerability	6.5	More Details
CVE-2022-38006	Windows Graphics Component Information Disclosure Vulnerability	6.5	More Details

CVE Number	Description	Base Score	Reference
CVE-2022-30312	The Trend Controls IC protocol through 2022-05-06 allows Cleartext Transmission of Sensitive Information. According to FSCT-2022-0050, there is a Trend Controls Inter-Controller (IC) protocol cleartext transmission of credentials issue. The affected components are characterized as: Inter-Controller (IC) protocol (57612/UDP). The potential impact is: Compromise of credentials. Several Trend Controls building automation controllers utilize the Inter-Controller (IC) protocol in for information exchange and automation purposes. This protocol offers authentication in the form of a 4-digit PIN in order to protect access to sensitive operations like strategy uploads and downloads as well as optional 0-30 character username and password protection for web page access protection. Both the PIN and usernames and passwords are transmitted in cleartext, allowing an attacker with passive interception capabilities to obtain these credentials. Credentials are transmitted in cleartext. An attacker who obtains Trend IC credentials can carry out sensitive engineering actions such as manipulating controller strategy or configuration settings. If the credentials in question are (re)used for other applications, their compromise could potentially facilitate lateral movement.	6.5	More Details
CVE-2022-35637	IBM Db2 for Linux, UNIX and Windows 9.7, 10.1, 10.5, 11.1, and 11.5 is vulnerable to a denial of service after entering a malformed SQL statement into the Db2expln tool. IBM X-Force ID: 230823.	6.5	More Details
CVE-2022-37959	Network Device Enrollment Service (NDES) Security Feature Bypass Vulnerability	6.5	More Details
CVE-2022-37191	The component "cuppa/api/index.php" of CuppaCMS v1.0 is Vulnerable to LFI. An authenticated user can read system files via crafted POST request using [function] parameter value as LFI payload.	6.5	More Details
CVE-2022-22483	IBM Db2 for Linux, UNIX and Windows 9.7, 10.1, 10.5, 11.1, and 11.5 is vulnerable to an information disclosure in some scenarios due to unauthorized access caused by improper privilege management when CREATE OR REPLACE command is used. IBM X-Force ID: 225979.	6.5	More Details
CVE-2021-44425	An issue was discovered in AnyDesk before 6.2.6 and 6.3.x before 6.3.3. An unnecessarily open listening port on a machine in the LAN of an attacker, opened by the Anydesk Windows client when using the tunneling feature, allows the attacker unauthorized access to the local machine's AnyDesk tunneling protocol stack (and also to any remote destination machine software that is listening to the AnyDesk tunneled port).	6.5	More Details
CVE-2022-31251	A Incorrect Default Permissions vulnerability in the packaging of the slurm testsuite of openSUSE Factory allows local attackers with control over the slurm user to escalate to root. This issue affects: openSUSE Factory slurm versions prior to 22.05.2-3.3.	6.5	More Details
CVE-2022-36107	TYPO3 is an open source PHP based web content management system released under the GNU GPL. It has been discovered that the `FileDumpController` (backend and frontend context) is vulnerable to cross-site scripting when malicious files are displayed using this component. A valid backend user account is needed to exploit this vulnerability. Update to TYPO3 version 7.6.58 ELTS, 8.7.48 ELTS, 9.5.37 ELTS, 10.4.32 or 11.5.16 that fix the problem. There are no known workarounds for this issue.	6.5	More Details
CVE-2022-36108	TYPO3 is an open source PHP based web content management system released under the GNU GPL. It has been discovered that the `f:asset.css` view helper is vulnerable to cross-site scripting when user input is passed as variables to the CSS. Update to TYPO3 version 10.4.32 or 11.5.16 that fix the problem. There are no known workarounds for this issue.	6.5	More Details
CVE-2022-31324	An arbitrary file download vulnerability in the downloadAction() function of Penta Security Systems Inc WAPPLES v6.0 r3 4.10-hotfix1 allows attackers to download arbitrary files via a crafted POST request.	6.5	More Details
CVE-2022-38266	An issue in the Leptonica linked library (v1.79.0) allows attackers to cause an arithmetic exception leading to a Denial of Service (DoS) via a crafted JPEG file.	6.5	More Details
CVE-2022-40635	Improper Control of Dynamically-Managed Code Resources vulnerability in Crafter Studio of Crafter CMS allows authenticated developers to execute OS commands via Groovy Sandbox Bypass.	6.4	More Details
CVE-2022-40634	Improper Control of Dynamically-Managed Code Resources vulnerability in Crafter Studio of Crafter CMS allows authenticated developers to execute OS commands via FreeMarker SSTI.	6.4	More Details

CVE Number	Description	Base Score	Reference
CVE-2022-38096	A NULL pointer dereference vulnerability was found in vmwgfx driver in drivers/gpu/vmxgfx/vmxgfx_execbuf.c in GPU component of Linux kernel with device file '/dev/dri/renderD128 (or Dxxx)'. This flaw allows a local attacker with a user account on the system to gain privilege, causing a denial of service(DoS).	6.3	More Details
CVE-2022-38457	A use-after-free(UAF) vulnerability was found in function 'vmw_cmd_res_check' in drivers/gpu/vmxgfx/vmxgfx_execbuf.c in Linux kernel's vmwgfx driver with device file '/dev/dri/renderD128 (or Dxxx)'. This flaw allows a local attacker with a user account on the system to gain privilege, causing a denial of service(DoS).	6.3	More Details
CVE-2022-36280	An out-of-bounds(OOB) memory access vulnerability was found in vmwgfx driver in drivers/gpu/vmxgfx/vmxgfx_kms.c in GPU component in the Linux kernel with device file '/dev/dri/renderD128 (or Dxxx)'. This flaw allows a local attacker with a user account on the system to gain privilege, causing a denial of service(DoS).	6.3	More Details
CVE-2022-3190	Infinite loop in the F5 Ethernet Trailer protocol dissector in Wireshark 3.6.0 to 3.6.7 and 3.4.0 to 3.4.15 allows denial of service via packet injection or crafted capture file	6.3	More Details
CVE-2022-40133	A use-after-free(UAF) vulnerability was found in function 'vmw_execbuf_tie_context' in drivers/gpu/vmxgfx/vmxgfx_execbuf.c in Linux kernel's vmwgfx driver with device file '/dev/dri/renderD128 (or Dxxx)'. This flaw allows a local attacker with a user account on the system to gain privilege, causing a denial of service(DoS).	6.3	More Details
CVE-2022-36109	Moby is an open-source project created by Docker to enable software containerization. A bug was found in Moby (Docker Engine) where supplementary groups are not set up properly. If an attacker has direct access to a container and manipulates their supplementary group access, they may be able to use supplementary group access to bypass primary group restrictions in some cases, potentially gaining access to sensitive information or gaining the ability to execute code in that container. This bug is fixed in Moby (Docker Engine) 20.10.18. Running containers should be stopped and restarted for the permissions to be fixed. For users unable to upgrade, this problem can be worked around by not using the `"USER $USERNAME"` Dockerfile instruction. Instead by calling `ENTRYPOINT ["su", "-", "user"]` the supplementary groups will be set up properly.	6.3	More Details
CVE-2022-36102	Shopware is an open source e-commerce software. In affected versions if backend admin controllers are called with a certain notation, the ACL could be bypassed. Users could execute actions, which they are normally not able to do. Users are advised to update to the current version (5.7.15). Users can get the update via the Auto-Updater or directly via the download overview. There are no known workarounds for this issue.	6.3	More Details
CVE-2022-3129	A vulnerability was found in codeprojects Online Driving School. It has been rated as critical. Affected by this issue is some unknown functionality of the file /registration.php. The manipulation 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-207872.	6.3	More Details
CVE-2022-38701	OpenHarmony-v3.1.2 and prior versions have a heap overflow vulnerability. Local attackers can trigger a heap overflow and get network sensitive information.	6.2	More Details
CVE-2022-39846	DLL hijacking vulnerability in Smart Switch PC prior to version 4.3.22083_3 allows attacker to execute arbitrary code.	6.2	More Details
CVE-2022-38081	OpenHarmony-v3.1.2 and prior versions have a permission bypass vulnerability. LAN attackers can bypass the distributed permission control.To take advantage of this weakness, attackers need another vulnerability to obtain system.	6.2	More Details
CVE-2022-38064	OpenHarmony-v3.1.2 and prior versions have a permission bypass vulnerability. Local attackers can bypass permission control and get sensitive information.	6.2	More Details
CVE-2022-35298	SAP NetWeaver Enterprise Portal (KMC) - version 7.50, does not sufficiently encode user-controlled inputs, resulting in Cross-Site Scripting vulnerability. KMC servlet is vulnerable to XSS attack. The execution of script content by a victim registered on the portal could compromise the confidentiality and integrity of victim’s web browser session.	6.1	More Details

CVE Number	Description	Base Score	Reference
CVE-2022-36020	The typo3/html-sanitizer package is an HTML sanitizer, written in PHP, aiming to provide XSS-safe markup based on explicitly allowed tags, attributes and values. Due to a parsing issue in the upstream package `masterminds/html5`, malicious markup used in a sequence with special HTML comments cannot be filtered and sanitized. This allows for a bypass of the cross-site scripting mechanism of `typo3/html-sanitizer`. This issue has been addressed in versions 1.0.7 and 2.0.16 of the `typo3/html-sanitizer` package. Users are advised to upgrade. There are no known workarounds for this issue.	6.1	More Details
CVE-2022-39799	An attacker with no prior authentication could craft and send malicious script to SAP GUI for HTML within Fiori Launchpad, resulting in reflected cross-site scripting attack. This could lead to stealing session information and impersonating the affected user.	6.1	More Details
CVE-2022-40323	SysAid Help Desk before 22.1.65 allows XSS in the Password Services module, aka FR# 67241.	6.1	More Details
CVE-2022-40322	SysAid Help Desk before 22.1.65 allows XSS, aka FR# 66542 and 65579.	6.1	More Details
CVE-2022-40324	SysAid Help Desk before 22.1.65 allows XSS via the Linked SRs field, aka FR# 67258.	6.1	More Details
CVE-2022-36736	Jitsi-2.10.5550 was discovered to contain a vulnerability in its web UI which allows attackers to perform a clickjacking attack via a crafted HTTP request. NOTE: this is disputed by the vendor	6.1	More Details
CVE-2022-39810	An issue was discovered in WSO2 Enterprise Integrator 6.4.0. A Reflected Cross-Site Scripting (XSS) vulnerability has been identified in the Management Console under /carbon/ndatasource/validateconnection/ajaxprocessor.jsp via the driver parameter. Session hijacking or similar attacks would not be possible.	6.1	More Details
CVE-2022-3138	Cross-site Scripting (XSS) - Generic in GitHub repository jgraph/drawio prior to 20.3.0.	6.1	More Details
CVE-2022-39814	In NOKIA 1350 OMS R14.2, an Open Redirect vulnerability occurs is the login page via next HTTP GET parameter.	6.1	More Details
CVE-2022-38254	Nagios XI before v5.8.7 was discovered to contain a cross-site scripting (XSS) vulnerability via the ajax.php script in CCM 3.1.5.	6.1	More Details
CVE-2022-38249	Nagios XI v5.8.6 was discovered to contain a cross-site scripting (XSS) vulnerability via the MTR component in version 1.0.4.	6.1	More Details
CVE-2022-38248	Nagios XI before v5.8.7 was discovered to contain multiple cross-site scripting (XSS) vulnerabilities at auditlog.php.	6.1	More Details
CVE-2022-3148	Cross-site Scripting (XSS) - Generic in GitHub repository jgraph/drawio prior to 20.3.0.	6.1	More Details
CVE-2022-39809	An issue was discovered in WSO2 Enterprise Integrator 6.4.0. A Reflected Cross-Site Scripting (XSS) vulnerability has been identified in the Management Console under /carbon/mediation_secure_vault/properties/ajaxprocessor.jsp via the name parameter. Session hijacking or similar attacks would not be possible.	6.1	More Details
CVE-2022-40325	SysAid Help Desk before 22.1.65 allows XSS via the Asset Dashboard, aka FR# 67262.	6.1	More Details

CVE Number	Description	Base Score	Reference
CVE-2020-19914	Cross Site Scripting (XSS) in xiunobbs 4.0.4 allows remote attackers to execute arbitrary web script or HTML via the attachment upload function.	6.1	More Details
CVE-2022-38972	Cross-site scripting vulnerability in Movable Type plugin A-Form versions prior to 4.1.1 (for Movable Type 7 Series) and versions prior to 3.9.1 (for Movable Type 6 Series) allows a remote unauthenticated attacker to inject an arbitrary script.	6.1	More Details
CVE-2022-36080	Wikmd is a file based wiki that uses markdown. Prior to version 1.7.1, an attacker could capture user's session cookies or execute malicious Javascript when a victim edits a markdown file. Version 1.7.1 fixes this issue.	6.1	More Details
CVE-2022-37731	ftcms 2.1 poster.PHP has a XSS vulnerability. The attacker inserts malicious JavaScript code into the web page, causing the user / administrator to trigger malicious code when accessing.	6.1	More Details
CVE-2022-38295	Cuppa CMS v1.0 was discovered to contain a cross-site scripting vulnerability at /table_manager/view/cu_user_groups. This vulnerability allows attackers to execute arbitrary web scripts or HTML via a crafted payload injected into the Name field under the Add New Group function.	6.1	More Details
CVE-2022-38291	SLiMS Senayan Library Management System v9.4.2 was discovered to contain a cross-site scripting (XSS) vulnerability via the Search function. This vulnerability allows attackers to execute arbitrary web scripts or HTML via a crafted payload injected into the Search bar.	6.1	More Details
CVE-2022-36867	Improper access control vulnerability in Editor Lite prior to version 4.0.40.14 allows attackers to access sensitive information.	5.9	More Details
CVE-2022-36873	Improper restriction of broadcasting Intent in GalaxyStoreBridgePageLinker of?Waterplugin prior to version 2.2.11.22081151 leaks MAC address of the connected Bluetooth device.	5.9	More Details
CVE-2022-36874	Improper Handling of Insufficient Permissions or Privileges vulnerability in Waterplugin prior to 2.2.11.22040751 allows attacker to access device IMEI and Serial number.	5.9	More Details
CVE-2022-36104	TYPO3 is an open source PHP based web content management system released under the GNU GPL. In affected versions requesting invalid or non-existing resources via HTTP triggers the page error handler which again could retrieve content to be shown as an error message from another page. This leads to a scenario in which the application is calling itself recursively - amplifying the impact of the initial attack until the limits of the web server are exceeded. Users are advised to update to TYPO3 version 11.5.16 to resolve this issue. There are no known workarounds for this issue.	5.9	More Details
CVE-2022-36861	Custom permission misuse vulnerability in SystemUI prior to SMR Sep-2022 Release 1 allows attacker to use some protected functions with SystemUI privilege.	5.9	More Details
CVE-2022-36782	Pal Electronics Systems - Pal Gate Authorization Errors. The vulnerability is an authorization problem in PalGate device management android client app. Gates of bulidings and parking lots with a simple button in any smartphone. The API was found after a decompiling and static research using Jadx, and a dynamic analasys using Frida. The attacker can iterate over all the IOT devices to see every entry and exit, on every gate and device all over the world, he can also scrape the server and create a user's DB with full names and phone number of over 2.8 million users, and to see all of the users' movement in and out of gates, even in real time.	5.9	More Details
CVE-2022-38400	Mailform Pro CGI 4.3.1 and earlier allow a remote unauthenticated attacker to obtain the user input data by having a use of the product to access a specially crafted URL.	5.9	More Details
CVE-2022-25897	The package org.eclipse.milo:sdk-server before 0.6.8 are vulnerable to Denial of Service (DoS) when bypassing the limitations for excessive memory consumption by sending multiple CloseSession requests with the deleteSubscription parameter equal to False.	5.9	More Details
CVE-2019-25076	The TSS (Tuple Space Search) algorithm in Open vSwitch 2.x through 2.17.2 and 3.0.0 allows remote attackers to cause a denial of service (delays of legitimate traffic) via crafted packet data that requires excessive evaluation time within the packet classification algorithm for the MegaFlow cache, aka a Tuple Space Explosion (TSE) attack.	5.8	More Details

CVE Number	Description	Base Score	Reference
CVE-2022-36859	Improper input validation vulnerability in SmartTagPlugin prior to version 1.2.21-6 allows privileged attackers to trigger a XSS on a victim's devices.	5.7	More Details
CVE-2022-36087	OAuthLib is an implementation of the OAuth request-signing logic for Python 3.6+. In OAuthLib versions 3.1.1 until 3.2.1, an attacker providing malicious redirect uri can cause denial of service. An attacker can also leverage usage of `uri_validate` functions depending where it is used. OAuthLib applications using OAuth2.0 provider support or use directly `uri_validate` are affected by this issue. Version 3.2.1 contains a patch. There are no known workarounds.	5.7	More Details
CVE-2022-3027	The CMS8000 device does not properly control or sanitize the SSID name of a new Wi-Fi access point. A threat actor could create an SSID with a malicious name, including non-standard characters that, when the device attempts connecting to the malicious SSID, the device can be exploited to write arbitrary files or display incorrect information.	5.7	More Details
CVE-2022-25914	The package com.google.cloud.tools:jib-core before 0.22.0 are vulnerable to Remote Code Execution (RCE) via the isDockerInstalled function, due to attempting to execute input.	5.6	More Details
CVE-2022-34728	Windows Graphics Component Information Disclosure Vulnerability	5.5	More Details
CVE-2022-38496	LIEF commit 365a16a was discovered to contain a reachable assertion abort via the component BinaryStream.hpp.	5.5	More Details
CVE-2022-35832	Windows Event Tracing Denial of Service Vulnerability	5.5	More Details
CVE-2022-38307	LIEF commit 5d1d643 was discovered to contain a segmentation violation via the function LIEF::MachO::SegmentCommand::file_offset() at /MachO/SegmentCommand.cpp.	5.5	More Details
CVE-2022-35831	Windows Remote Access Connection Manager Information Disclosure Vulnerability	5.5	More Details
CVE-2022-38497	LIEF commit 365a16a was discovered to contain a segmentation violation via the component CoreFile.tcc:69.	5.5	More Details
CVE-2022-2905	An out-of-bounds memory read flaw was found in the Linux kernel's BPF subsystem in how a user calls the bpf_tail_call function with a key larger than the max_entries of the map. This flaw allows a local user to gain unauthorized access to data.	5.5	More Details
CVE-2022-26394	The Baxter Spectrum WBM does not perform mutual authentication with the gateway server host. This may allow an attacker to perform a man in the middle attack that modifies parameters making the network connection fail.	5.5	More Details
CVE-2022-34723	Windows DPAPI (Data Protection Application Programming Interface) Information Disclosure Vulnerability	5.5	More Details
CVE-2022-3153	NULL Pointer Dereference in GitHub repository vim/vim prior to 9.0.0404.	5.5	More Details
CVE-2022-20396	In SettingsActivity.java, there is a possible way to make a device discoverable over Bluetooth, without permission or user interaction, due to a permissions bypass. This could lead to local escalation of privilege with no additional execution privileges needed. User interaction is not needed for exploitation.Product: AndroidVersions: Android-12L Android-13Android ID: A-234440688	5.5	More Details
CVE-2022-20399	In the SEPolicy configuration of system apps, there is a possible access to the 'ip' utility due to an insecure default value. This could lead to local information disclosure of network data with no additional execution privileges needed. User interaction is not needed for exploitation.Product: AndroidVersions: Android kernelAndroid ID: A-219808546References: Upstream kernel	5.5	More Details

CVE Number	Description	Base Score	Reference
CVE-2022-37302	A CWE-119: Improper Restriction of Operations within the Bounds of a Memory Buffer vulnerability exists that could cause a crash of the Control Expert software when an incorrect project file is opened. Affected Products: EcoStruxure Control Expert(V15.1 HF001 and prior).	5.5	More Details
CVE-2022-3077	A buffer overflow vulnerability was found in the Linux kernel Intel's iSMT SMBus host controller driver in the way it handled the I2C_SMBUS_BLOCK_PROC_CALL case (via the ioctl I2C_SMBUS) with malicious input data. This flaw could allow a local user to crash the system.	5.5	More Details
CVE-2022-34110	An issue in Micro-Star International MSI Feature Navigator v1.0.1808.0901 allows attackers to download arbitrary files regardless of file type or size.	5.5	More Details
CVE-2022-3169	A flaw was found in the Linux kernel. A denial of service flaw may occur if there is a consecutive request of the NVME_IOCTL_RESET and the NVME_IOCTL_SUBSYS_RESET through the device file of the driver, resulting in a PCIe link disconnect.	5.5	More Details
CVE-2021-40647	In man2html 1.6g, a specific string being read in from a file will overwrite the size parameter in the top chunk of the heap. This at least causes the program to segmentation abort if the heap size parameter isn't aligned correctly. In version before GLIBC version 2.29 and aligned correctly, it allows arbitrary write anywhere in the programs memory.	5.5	More Details
CVE-2021-40648	In man2html 1.6g, a filename can be created to overwrite the previous size parameter of the next chunk and the fd, bk, fd_nextsize, bk_nextsize of the current chunk. The next chunk is then freed later on, causing a freeing of an arbitrary amount of memory.	5.5	More Details
CVE-2022-1602	A potential security vulnerability has been identified in HP ThinPro 7.2 Service Pack 8 (SP8). The security vulnerability in SP8 is not remedied after upgrading from SP8 to Service Pack 9 (SP9). HP has released Service Pack 10 (SP10) to remediate the potential vulnerability introduced in SP8.	5.5	More Details
CVE-2022-39845	Improper validation of integrity check vulnerability in Samsung Kies prior to version 2.6.4.22074 allows local attackers to delete arbitrary directory using directory junction.	5.5	More Details
CVE-2022-39844	Improper validation of integrity check vulnerability in Smart Switch PC prior to version 4.3.22083 allows local attackers to delete arbitrary directory using directory junction.	5.5	More Details
CVE-2022-38059	Cross-Site Request Forgery (CSRF) vulnerability in Alexey Trofimov's Access Code Feeder plugin <= 1.0.3 at WordPress.	5.5	More Details
CVE-2022-20393	In extract3GPPGlobalDescriptions of TextDescriptions.cpp, there is a possible out of bounds read due to an integer overflow. This could lead to local information disclosure from the media server with no additional execution privileges needed. User interaction is not needed for exploitation.Product: AndroidVersions: Android-11 Android-12 Android-12LAndroid ID: A-233735886	5.5	More Details
CVE-2022-37796	In Simple Online Book Store System 1.0 in /admin_book.php the Title, Author, and Description parameters are vulnerable to Cross Site Scripting(XSS).	5.4	More Details
CVE-2022-34165	IBM WebSphere Application Server 7.0, 8.0, 8.5, and 9.0 and IBM WebSphere Application Server Liberty 17.0.0.3 through 22.0.0.9 are vulnerable to HTTP header injection, caused by improper validation. This could allow an attacker to conduct various attacks against the vulnerable system, including cache poisoning and cross-site scripting. IBM X-Force ID: 229429.	5.4	More Details
CVE-2022-25295	This affects the package github.com/gophish/gophish before 0.12.0. The Open Redirect vulnerability exists in the next query parameter. The application uses url.Parse(r.FormValue("next")) to extract path and eventually redirect user to a relative URL, but if next parameter starts with multiple backslashes like \\\\\\example.com, browser will redirect user to http://example.com.	5.4	More Details
CVE-2022-38639	A cross-site scripting (XSS) vulnerability in Markdown-Nice v1.8.22 allows attackers to execute arbitrary web scripts or HTML via a crafted payload injected into the Community Posting field.	5.4	More Details

CVE Number	Description	Base Score	Reference
CVE-2022-38139	Multiple Cross-Site Request Forgery (CSRF) vulnerabilities in RD Station plugin <= 5.2.0 at WordPress.	5.4	More Details
CVE-2022-36254	Multiple persistent cross-site scripting (XSS) vulnerabilities in index.php in tramyardg Hotel Management System 1.0 allow remote attackers to inject arbitrary web script or HTML via multiple parameters such as "fullname".	5.4	More Details
CVE-2022-36101	Shopware is an open source e-commerce software. In affected versions the request for the customer detail view in the backend administration contained sensitive data like the hashed password and the session ID. These fields are now explicitly unset in version 5.7.15. Users are advised to update and may get the update either via the Auto-Updater or directly via the download overview. There are no known workarounds for this issue.	5.4	More Details
CVE-2022-38135	Broken Access Control vulnerability in Dean Oakley's Photospace Gallery plugin <= 2.3.5 at WordPress allows users with subscriber or higher role to change plugin settings.	5.4	More Details
CVE-2022-40317	OpenKM 6.3.11 allows stored XSS related to the javascript: substring in an A element.	5.4	More Details
CVE-2022-36106	TYPO3 is an open source PHP based web content management system released under the GNU GPL. It has been discovered that the expiration time of a password reset link for TYPO3 backend users has never been evaluated. As a result, a password reset link could be used to perform a password reset even if the default expiry time of two hours has been exceeded. Update to TYPO3 version 10.4.32 or 11.5.16 that fix the problem. There are no known workarounds for this issue.	5.4	More Details
CVE-2022-40191	Authenticated (subscriber+) Stored Cross-Site Scripting (XSS) vulnerability in Ali Khallad's Contact Form By Mega Forms plugin <= 1.2.4 at WordPress.	5.4	More Details
CVE-2022-31861	Cross site Scripting (XSS) in ThingsBoard IoT Platform through 3.3.4.1 via a crafted value being sent to the audit logs.	5.4	More Details
CVE-2021-36568	In certain Moodle products after creating a course, it is possible to add in a arbitrary "Topic" a resource, in this case a "Database" with the type "Text" where its values "Field name" and "Field description" are vulnerable to Cross Site Scripting Stored(XSS). This affects Moodle 3.11 and Moodle 3.10.4 and Moodle 3.9.7.	5.4	More Details
CVE-2022-35294	An attacker with basic business user privileges could craft and upload a malicious file to SAP NetWeaver Application Server ABAP, which is then downloaded and viewed by other users resulting in a stored Cross-Site-Scripting attack. This could lead to information disclosure including stealing authentication information and impersonating the affected user.	5.4	More Details
CVE-2022-38256	TastyIgniter v3.5.0 was discovered to contain a cross-site scripting (XSS) vulnerability which allows attackers to execute arbitrary web scripts or HTML via a crafted payload.	5.4	More Details
CVE-2022-2925	Cross-site Scripting (XSS) - Stored in GitHub repository appwrite/appwrite prior to 1.0.0-RC1.	5.4	More Details
CVE-2022-38093	Multiple Cross-Site Request Forgery (CSRF) vulnerabilities in All in One SEO plugin <= 4.2.3.1 at WordPress.	5.4	More Details
CVE-2022-35277	Cross-Site Request Forgery (CSRF) vulnerability in GetResponse plugin <= 5.5.20 at WordPress.	5.4	More Details
CVE-2022-37411	Cross-Site Request Forgery (CSRF) vulnerability in Vinoj Cardoza's Captcha Code plugin <= 2.7 at WordPress.	5.4	More Details

CVE Number	Description	Base Score	Reference
CVE-2022-39207	Onedev is an open source, self-hosted Git Server with CI/CD and Kanban. During CI/CD builds, it is possible to save build artifacts for later retrieval. They can be accessed through OneDev's web UI after the successful run of a build. These artifact files are served by the webserver in the same context as the UI without any further restrictions. This leads to Cross-Site Scripting (XSS) when a user creates a build artifact that contains HTML. When accessing the artifact, the content is rendered by the browser, including any JavaScript that it contains. Since all cookies (except for the rememberMe one) do not set the HttpOnly flag, an attacker could steal the session of a victim and use it to impersonate them. To exploit this issue, attackers need to be able to modify the content of artifacts, which usually means they need to be able to modify a project's build spec. The exploitation requires the victim to click on an attacker's link. It can be used to elevate privileges by targeting admins of a OneDev instance. In the worst case, this can lead to arbitrary code execution on the server, because admins can create Server Shell Executors and use them to run any command on the server. This issue has been patched in version 7.3.0. Users are advised to upgrade. There are no known workarounds for this issue.	5.4	More Details
CVE-2022-34336	IBM WebSphere Application Server 7.0, 8.0, 8.5, and 9.0 is vulnerable to cross-site scripting. This vulnerability allows users to embed arbitrary JavaScript code in the Web UI thus altering the intended functionality potentially leading to credentials disclosure within a trusted session. IBM X-Force ID: 229714.	5.4	More Details
CVE-2022-38070	Privilege Escalation (subscriber+) vulnerability in Pop-up plugin <= 1.1.5 at WordPress.	5.4	More Details
CVE-2022-22330	IBM Control Desk 7.6.1 could allow a remote attacker to obtain sensitive information, caused by the failure to set the HTTPOnly flag. A remote attacker could exploit this vulnerability to obtain sensitive information from the cookie. IBM X-Force ID: 219126.	5.3	More Details
CVE-2022-21950	A Improper Access Control vulnerability in the systemd service of cana in openSUSE Backports SLE-15-SP3, openSUSE Backports SLE-15-SP4 allows local users to hijack the UNIX domain socket This issue affects: openSUSE Backports SLE-15-SP3 canna versions prior to canna-3.7p3-bp153.2.3.1. openSUSE Backports SLE-15-SP4 canna versions prior to 3.7p3-bp154.3.3.1. openSUSE Factory was also affected. Instead of fixing the package it was deleted there.	5.3	More Details
CVE-2022-38770	The mobile application in Transtek Mojodat FAM (Fixed Asset Management) 2.4.6 allows remote attackers to fetch other users' data upon a successful login request.	5.3	More Details
CVE-2022-37146	The PlexTrac platform prior to version 1.28.0 allows for username enumeration via HTTP response times on invalid login attempts for users configured to use the PlexTrac authentication provider. Login attempts for valid, unlocked users configured to use PlexTrac as their authentication provider take significantly longer than those for invalid users, allowing for valid users to be enumerated by an unauthenticated remote attacker. Note that the lockout policy implemented in Plextrac version 1.17.0 makes it impossible to distinguish between valid, locked user accounts and user accounts that do not exist, but does not prevent valid, unlocked users from being enumerated.	5.3	More Details
CVE-2022-39014	Under certain conditions SAP BusinessObjects Business Intelligence Platform Central Management Console (CMC) - version 430, allows an attacker to access certain unencrypted sensitive parameters which would otherwise be restricted.	5.3	More Details
CVE-2022-36105	TYPO3 is an open source PHP based web content management system released under the GNU GPL. It has been discovered that observing response time during user authentication (backend and frontend) can be used to distinguish between existing and non-existing user accounts. Extension authors of 3rd party TYPO3 extensions providing a custom authentication service should check if the extension is affected by the described problem. Affected extensions must implement new `MimicServiceInterface::mimicAuthUser`, which simulates corresponding times regular processing would usually take. Update to TYPO3 version 7.6.58 ELTS, 8.7.48 ELTS, 9.5.37 ELTS, 10.4.32 or 11.5.16 that fix this problem. There are no known workarounds for this issue.	5.3	More Details
CVE-2022-36082	mangadex-downloader is a command-line tool to download manga from MangaDex. When using `file:<location>` command and `<location>` is a web URL location (http, https), mangadex-downloader between versions 1.3.0 and 1.7.2 will try to open and read a file in local disk for each line of website contents. Version 1.7.2 contains a patch for this issue.	5.3	More Details

CVE Number	Description	Base Score	Reference
CVE-2022-36083	JOSE is "JSON Web Almost Everything" - JWA, JWS, JWE, JWT, JWK, JWKS with no dependencies using runtime's native crypto in Node.js, Browser, Cloudflare Workers, Electron, and Deno. The PBKDF2-based JWE key management algorithms expect a JOSE Header Parameter named `p2c` PBES2 Count, which determines how many PBKDF2 iterations must be executed in order to derive a CEK wrapping key. The purpose of this parameter is to intentionally slow down the key derivation function in order to make password brute-force and dictionary attacks more expensive. This makes the PBES2 algorithms unsuitable for situations where the JWE is coming from an untrusted source: an adversary can intentionally pick an extremely high PBES2 Count value, that will initiate a CPU-bound computation that may take an unreasonable amount of time to finish. Under certain conditions, it is possible to have the user's environment consume unreasonable amount of CPU time. The impact is limited only to users utilizing the JWE decryption APIs with symmetric secrets to decrypt JWEs from untrusted parties who do not limit the accepted JWE Key Management Algorithms (`alg` Header Parameter) using the `keyManagementAlgorithms` (or `algorithms` in v1.x) decryption option or through other means. The `v1.28.2`, `v2.0.6`, `v3.20.4`, and `v4.9.2` releases limit the maximum PBKDF2 iteration count to `10000` by default. It is possible to adjust this limit with a newly introduced `maxPBES2Count` decryption option. If users are unable to upgrade their required library version, they have two options depending on whether they expect to receive JWEs using any of the three PBKDF2-based JWE key management algorithms. They can use the `keyManagementAlgorithms` decryption option to disable accepting PBKDF2 altogether, or they can inspect the JOSE Header prior to using the decryption API and limit the PBKDF2 iteration count (`p2c` Header Parameter).	5.3	More Details
CVE-2022-26049	This affects the package com.diffplug.gradle:goomph before 3.37.2. It allows a malicious zip file to potentially break out of the expected destination directory, writing contents into arbitrary locations on the file system. Overwriting certain files/directories could allow an attacker to achieve remote code execution on a target system by exploiting this vulnerability. **Note:** This could have allowed a malicious zip file to extract itself into an arbitrary directory. The only file that Goomph extracts is the p2 bootstrapper and eclipse metadata files hosted at eclipse.org, which are not malicious, so the only way this vulnerability could have affected you is if you had set a custom bootstrap zip, and that zip was malicious.	5.3	More Details
CVE-2022-3175	Missing Custom Error Page in GitHub repository ikus060/rdiffweb prior to 2.4.2.	5.3	More Details
CVE-2022-39158	Affected devices improperly handle partial HTTP requests which makes them vulnerable to slowloris attacks. This could allow a remote attacker to create a denial of service condition that persists until the attack ends.	5.3	More Details
CVE-2022-27969	Cynet 360 Web Portal before v4.5 was discovered to allow attackers to access a list of decoy users via a crafted GET request sent to /WebApp/DeceptionUser/GetAllDeceptionUsers.	5.3	More Details
CVE-2022-27968	Cynet 360 Web Portal before v4.5 was discovered to allow attackers to access a list of monitored files and profiles via a crafted GET request sent to /WebApp/SettingsFileMonitor/GetFileMonitorProfiles.	5.3	More Details
CVE-2022-27967	Cynet 360 Web Portal before v4.5 was discovered to allow attackers to access a list of excluded files and profiles via a crafted GET request sent to /WebApp/SettingsExclusion/GetExclusionsProfiles.	5.3	More Details
CVE-2022-32244	Under certain conditions an attacker authenticated as a CMS administrator access the BOE Commentary database and retrieve (non-personal) system data, modify system data but can't make the system unavailable. This needs the attacker to have high privilege access to the same physical/logical network to access information which would otherwise be restricted, leading to low impact on confidentiality and high impact on integrity of the application.	5.2	More Details
CVE-2022-36848	Improper Authorization vulnerability in setDualDARPolicyCmd prior to SMR Sep-2022 Release 1 allows local attackers to cause local permanent denial of service.	5.1	More Details
CVE-2022-36088	GoCD is a continuous delivery server. Windows installations via either the server or agent installers for GoCD prior to 22.2.0 do not adequately restrict permissions when installing outside of the default location. This could allow a malicious user with local access to the server GoCD Server or Agent are installed on to modify executables or components of the installation. This does not affect zip file-based installs, installations to other platforms, or installations inside `Program Files` or `Program Files (x86)`. This issue is fixed in GoCD 22.2.0 installers. As a workaround, if the server or agent is installed outside of `Program Files (x86)`, verify the the permission of the Server or Agent installation directory to ensure the `Everyone` user group does not have `Full Control`, `Modify` or `Write` permissions.	5.0	More Details

CVE Number	Description	Base Score	Reference
CVE-2022-26393	The Baxter Spectrum WBM is susceptible to format string attacks via application messaging. An attacker could use this to read memory in the WBM to access sensitive information or cause a Denial of Service (DoS) on the WBM.	5.0	More Details
CVE-2022-36870	Pending Intent hijacking vulnerability in MTransferNotificationManager in Samsung Pay prior to version 5.0.63 for KR and 5.1.47 for Global allows attackers to access files without permission via implicit Intent.	5.0	More Details
CVE-2022-36871	Pending Intent hijacking vulnerability in NotiCenterUtils in Samsung Pay prior to version 5.0.63 for KR and 5.1.47 for Global allows attackers to access files without permission via implicit Intent.	5.0	More Details
CVE-2022-36872	Pending Intent hijacking vulnerability in SpayNotification in Samsung Pay prior to version 5.0.63 for KR and 5.1.47 for Global allows attackers to access files without permission via implicit Intent.	5.0	More Details
CVE-2022-36849	Use after free vulnerability in sdp_mm_set_process_sensitive function of sdpmm driver prior to SMR Sep-2022 Release 1 allows attackers to perform malicious actions.	4.9	More Details
CVE-2022-36780	Avdor CIS - crystal quality Credentials Management Errors. The product is phone call recorder, you can hear all the recorded calls without authenticate to the system. Attacker sends crafted URL to the system: ip:port//V=2;ChannelID=number;Ext=number;Command=startLM;Client=number;Request=number;R=number number - id of the recorded number.	4.9	More Details
CVE-2022-36617	Arq Backup 7.19.5.0 and below stores backup encryption passwords using reversible encryption. This issue allows attackers with administrative privileges to recover cleartext passwords.	4.9	More Details
CVE-2022-36847	Use after free vulnerability in mtp_send_signal function of MTP driver prior to SMR Sep-2022 Release 1 allows attackers to perform malicious actions.	4.9	More Details
CVE-2022-35295	In SAP Host Agent (SAPOSCOL) - version 7.22, an attacker may use files created by saposcol to escalate privileges for themselves.	4.9	More Details
CVE-2022-37335	Authenticated (author+) Stored Cross-Site Scripting (XSS) vulnerability in WHA's Word Search Puzzles game plugin <= 2.0.1 at WordPress.	4.8	More Details
CVE-2022-38251	Nagios XI v5.8.6 was discovered to contain a cross-site scripting (XSS) vulnerability via the System Performance Settings page under the Admin panel.	4.8	More Details
CVE-2022-36356	Authenticated (admin+) Stored Cross-Site Scripting (XSS) vulnerability in Liam Gladdy / Thirty8 Digital Culture Object plugin <= 4.0.1 at WordPress.	4.8	More Details
CVE-2022-37403	Authenticated (admin+) Stored Cross-Site Scripting (XSS) vulnerability in Nikhil Vaghela's Add User Role plugin <= 0.0.1 at WordPress.	4.8	More Details
CVE-2022-37404	Authenticated (admin+) Stored Cross-Site Scripting (XSS) vulnerability in Christian Salazar's add2fav plugin <= 1.0 at WordPress.	4.8	More Details
CVE-2022-35725	Authenticated (admin+) Stored Cross-Site Scripting (XSS) vulnerability in Hans Matzen's wp-forecast plugin <= 7.5 at WordPress.	4.8	More Details
CVE-2022-35275	Authenticated (shop manager+) Reflected Cross-Site Scripting (XSS) vulnerability in AlgolPlus Advanced Order Export For WooCommerce plugin <= 3.3.1 at WordPress.	4.8	More Details

CVE Number	Description	Base Score	Reference
CVE-2022-38068	Authenticated (admin+) Stored Cross-Site Scripting (XSS) vulnerability in Apasionados Export Post Info plugin <= 1.1.0 at WordPress.	4.8	More Details
CVE-2022-38247	Nagios XI v5.8.6 was discovered to contain a cross-site scripting (XSS) vulnerability via the System Settings page under the Admin panel.	4.8	More Details
CVE-2022-37412	Authenticated (admin+) Reflected Cross-Site Scripting (XSS) vulnerability in Galerio & Urda's Better Delete Revision plugin <= 1.6.1 at WordPress.	4.8	More Details
CVE-2022-40307	An issue was discovered in the Linux kernel through 5.19.8. drivers/firmware/efi/capsule-loader.c has a race condition with a resultant use-after-free.	4.7	More Details
CVE-2022-3205	Cross site scripting in automation controller UI in Red Hat Ansible Automation Platform 1.2 and 2.0 where the project name is susceptible to XSS injection	4.6	More Details
CVE-2022-36841	A heap-based overflow vulnerability in PrepareRecogLibrary_Part function in libSDKRecognitionText.spensdk.samsung.so library prior to SMR Sep-2022 Release 1 allows attacker to cause memory access fault.	4.4	More Details
CVE-2022-36842	A heap-based overflow vulnerability in prepareRecogLibrary function in libSDKRecognitionText.spensdk.samsung.so library prior to SMR Sep-2022 Release 1 allows attacker to cause memory access fault.	4.4	More Details
CVE-2022-36843	A heap-based overflow vulnerability in MHW_RECOG_LIB_INFO function in libSDKRecognitionText.spensdk.samsung.so library prior to SMR Sep-2022 Release 1 allows attacker to cause memory access fault.	4.4	More Details
CVE-2022-36844	A heap-based overflow vulnerability in HWR::EngJudgeModel::Construct() in libSDKRecognitionText.spensdk.samsung.so library prior to SMR Sep-2022 Release 1 allows attacker to cause memory access fault.	4.4	More Details
CVE-2022-36845	A heap-based overflow vulnerability in MHW_RECOG_LIB_INFO function in libSDKRecognitionText.spensdk.samsung.so library prior to SMR Sep-2022 Release 1 allows attacker to cause memory access fault.	4.4	More Details
CVE-2022-36846	A heap-based overflow vulnerability in ConstructDictionary function in libSDKRecognitionText.spensdk.samsung.so library prior to SMR Sep-2022 Release 1 allows attacker to cause memory access fault.	4.4	More Details
CVE-2022-36855	A use after free vulnerability in iva_ctl driver prior to SMR Sep-2022 Release 1 allows attacker to cause memory access fault.	4.4	More Details
CVE-2022-36858	A heap-based overflow vulnerability in GetCorrectDbLanguageTypeEsPKc() function in libSDKRecognitionText.spensdk.samsung.so library prior to SMR Sep-2022 Release 1 allows attacker to cause memory access fault.	4.4	More Details
CVE-2022-36863	A heap-based overflow vulnerability in GetCorrectDbLanguageTypeEsPKc function in libSDKRecognitionText.spensdk.samsung.so library prior to SMR Sep-2022 Release 1 allows attacker to cause memory access fault.	4.4	More Details
CVE-2022-36862	A heap-based overflow vulnerability in HWR::EngineCJK::Impl::Construct() in libSDKRecognitionText.spensdk.samsung.so library prior to SMR Sep-2022 Release 1 allows attacker to cause memory access fault.	4.4	More Details
CVE-2022-36860	A heap-based overflow vulnerability in LoadEnvironment function in libSDKRecognitionText.spensdk.samsung.so library prior to SMR Sep-2022 Release 1 allows attacker to cause memory access fault.	4.4	More Details

CVE Number	Description	Base Score	Reference
CVE-2022-36422	Rating increase/decrease via race condition in Lester 'GaMerZ' Chan WP-PostRatings plugin <= 1.89 at WordPress.	4.3	More Details
CVE-2022-38329	An issue was discovered in Shopxian CMS 3.0.0. There is a CSRF vulnerability that can delete the specified column via index.php/contents-admin_cat-finderdel-model-ContentsCat.html?id=17.	4.3	More Details
CVE-2022-37405	Cross-Site Request Forgery (CSRF) vulnerability in Mickey Kay's Better Font Awesome plugin <= 2.0.1 at WordPress.	4.3	More Details
CVE-2022-38058	Authenticated (subscriber+) Plugin Setting change vulnerability in WP Shamsi plugin <= 4.1.1 at WordPress.	4.3	More Details
CVE-2022-39202	matrix-appservice-irc is an open source Node.js IRC bridge for Matrix. The Internet Relay Chat (IRC) protocol allows you to specify multiple modes in a single mode command. Due to a bug in the underlying matrix-org/node-irc library, affected versions of matrix-appservice-irc perform parsing of such modes incorrectly, potentially resulting in the wrong user being given permissions. Mode commands can only be executed by privileged users, so this can only be abused if an operator is tricked into running the command on behalf of an attacker. The vulnerability has been patched in matrix-appservice-irc 0.35.0. As a workaround users should refrain from entering mode commands suggested by untrusted users. Avoid using multiple modes in a single command.	4.3	More Details
CVE-2022-22329	IBM Control Desk 7.6.1 does not set the secure attribute on authorization tokens or session cookies. Attackers may be able to get the cookie values by sending a http:// link to a user or by planting this link in a site the user goes to. The cookie will be sent to the insecure link and the attacker can then obtain the cookie value by snooping the traffic. IBM X-Force ID: 219124.	4.3	More Details
CVE-2022-36095	XWiki Platform is a generic wiki platform. Prior to versions 13.10.5 and 14.3, it is possible to perform a Cross-Site Request Forgery (CSRF) attack for adding or removing tags on XWiki pages. The problem has been patched in XWiki 13.10.5 and 14.3. As a workaround, one may locally modify the `documentTags.vm` template in one's filesystem, to apply the changes exposed there.	4.3	More Details
CVE-2022-20863	A vulnerability in the messaging interface of Cisco Webex App, formerly Webex Teams, could allow an unauthenticated, remote attacker to manipulate links or other content within the messaging interface. This vulnerability exists because the affected software does not properly handle character rendering. An attacker could exploit this vulnerability by sending messages within the application interface. A successful exploit could allow the attacker to modify the display of links or other content within the interface, potentially allowing the attacker to conduct phishing or spoofing attacks.	4.3	More Details
CVE-2022-38299	An issue in the Elasticsearch plugin of Appsmith v1.7.11 allows attackers to connect disallowed hosts to the AWS/GCP internal metadata endpoint.	4.3	More Details
CVE-2022-38069	Multiple globally default credentials exist across all CMS8000 devices, that once exposed, allow a threat actor with momentary physical access to gain privileged access to any device. Privileged credential access enables the extraction of sensitive patient information or modification of device parameters	4.3	More Details
CVE-2022-26390	The Baxter Spectrum Wireless Battery Module (WBM) stores network credentials and PHI (only applicable to Spectrum IQ pumps using auto programming) in unencrypted form. An attacker with physical access to a device that hasn't had all data and settings erased may be able to extract sensitive information.	4.2	More Details
CVE-2022-37407	Multiple Authenticated Stored Cross-Site Scripting (XSS) vulnerabilities in WPChill Gallery PhotoBlocks plugin <= 1.2.6 at WordPress.	4.1	More Details
CVE-2022-20923	A vulnerability in the IPSec VPN Server authentication functionality of Cisco Small Business RV110W, RV130, RV130W, and RV215W Routers could allow an unauthenticated, remote attacker to bypass authentication controls and access the IPSec VPN network. This vulnerability is due to the improper implementation of the password validation algorithm. An attacker could exploit this vulnerability by logging in to the VPN from an affected device with crafted credentials. A successful exploit could allow the attacker to bypass authentication and access the IPSec VPN network. The attacker may obtain privileges that are the same level as an administrative user, depending on the crafted credentials that are used. Cisco has not released software updates that address this vulnerability.	4.0	More Details

CVE Number	Description	Base Score	Reference
CVE-2022-36856	Improper access control vulnerability in Telecom application prior to SMR Sep-2022 Release 1 allows attacker to start emergency calls via undefined permission.	4.0	More Details
CVE-2022-36854	Out of bound read in libapexjni.media.samsung.so prior to SMR Sep-2022 Release 1 allows attacker access unauthorized information.	4.0	More Details
CVE-2022-36866	Improper access control vulnerability in Broadcaster in Group Sharing prior to versions 13.0.6.15 in Android S(12), 13.0.6.14 in Android R(11) and below allows attackers to identify the device.	4.0	More Details
CVE-2022-36865	Improper access control in Group Sharing prior to versions 13.0.6.15 in Android S(12), 13.0.6.14 in Android R(11) and below allows attackers to access device information.	4.0	More Details
CVE-2022-36864	Improper access control and intent redirection in Samsung Email prior to 6.1.70.20 allows attacker to access specific formatted file and execute privileged behavior.	4.0	More Details
CVE-2022-36850	Path traversal vulnerability in CallBGProvider prior to SMR Sep-2022 Release 1 allows attacker to overwrite arbitrary file with phone uid.	4.0	More Details
CVE-2022-36851	Improper access control vulnerability in Samsung pass prior to version 4.0.03.1 allow physical attackers to access data of Samsung pass on a certain state of an unlocked device.	3.9	More Details
CVE-2022-36878	Exposure of Sensitive Information in Find My Mobile prior to version 7.2.25.14 allows local attacker to access IMEI via log.	3.3	More Details
CVE-2022-36853	Intent redirection in Photo Editor prior to SMR Sep-2022 Release 1 allows attacker to get sensitive information.	3.3	More Details
CVE-2022-37703	In Amanda 3.5.1, an information leak vulnerability was found in the calcsize SUID binary. An attacker can abuse this vulnerability to know if a directory exists or not anywhere in the fs. The binary will use `opendir()` as root directly without checking the path, letting the attacker provide an arbitrary path.	3.3	More Details
CVE-2022-22314	IBM Planning Analytics Local 2.0 allows web pages to be stored locally which can be read by another user on the system. IBM X-Force ID: 217371.	3.3	More Details
CVE-2022-26392	The Baxter Spectrum WBM (v16, v16D38) and Baxter Spectrum WBM (v17, v17D19, v20D29 to v20D32) when in superuser mode is susceptible to format string attacks via application messaging. An attacker could use this to read memory in the WBM to access sensitive information.	3.1	More Details
CVE-2022-3147	Mattermost version 7.0.x and earlier fails to sufficiently limit the in-memory sizes of concurrently uploaded JPEG images, which allows authenticated users to cause resource exhaustion on specific system configurations, resulting in server-side Denial of Service.	3.1	More Details
CVE-2022-31225	Dell BIOS versions contain an Unchecked Return Value vulnerability. A local authenticated administrator user could potentially exploit this vulnerability in order to change the state of the system or cause unexpected failures.	3.0	More Details
CVE-2022-38453	Multiple binary application files on the CMS8000 device are compiled with 'not stripped' and 'debug_info' compilation settings. These compiler settings greatly decrease the level of effort for a threat actor to reverse engineer sensitive code and identify additional vulnerabilities.	3.0	More Details
CVE-2022-31220	Dell BIOS versions contain an Unchecked Return Value vulnerability. A local authenticated administrator user could potentially exploit this vulnerability in order to change the state of the system or cause unexpected failures.	3.0	More Details

CVE Number	Description	Base Score	Reference
CVE-2022-36877	Exposure of Sensitive Information in FaqSymptomCardViewModel in Samsung Members prior to versions 4.3.00.11 in Global and 14.0.02.4 in China allows local attackers to access device identification via log.	2.8	More Details
CVE-2022-31223	Dell BIOS versions contain an Improper Neutralization of Null Byte vulnerability. A local authenticated administrator user could potentially exploit this vulnerability by sending unexpected null bytes in order to read memory on the system.	2.3	More Details
CVE-2022-31221	Dell BIOS versions contain an Information Exposure vulnerability. A local authenticated administrator user could potentially exploit this vulnerability in order access sensitive state information on the system.	2.3	More Details
CVE-2022-31222	Dell BIOS versions contain a Missing Release of Resource after Effective Lifetime vulnerability. A local authenticated administrator user could potentially exploit this vulnerability by consuming excess memory in order to cause the application to crash.	2.3	More Details
CVE-2022-31224	Dell BIOS versions contain an Improper Protection Against Voltage and Clock Glitches vulnerability. An attacker with physical access to the system could potentially exploit this vulnerability by triggering a fault condition in order to change the behavior of the system.	2.0	More Details
CVE-2022-36852	Improper Authorization vulnerability in Video Editor prior to SMR Sep-2022 Release 1 allows local attacker to access internal application data.	1.9	More Details
CVE-2022-36857	Improper Authorization vulnerability in Photo Editor prior to SMR Sep-2022 Release 1 allows physical attackers to read internal application data.	1.9	More Details
CVE-2022-36876	Improper authorization in UPI payment in Samsung Pass prior to version 4.0.04.10 allows physical attackers to access account list without authentication.	1.8	More Details