SingCERT
Singapore Cyber Emergency Response Team

Security Bulletin 11 January 2023

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

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

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

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

CRITICAL VULNERABILITIES

CVE Number	Description	Base Score	Reference
CVE-2023-0018	Due to improper input sanitization of user-controlled input in SAP BusinessObjects Business Intelligence Platform CMC application - versions 420, and 430, an attacker with basic user-level privileges can modify/upload crystal reports containing a malicious payload. Once these reports are viewable, anyone who opens those reports would be susceptible to stored XSS attacks. As a result of the attack, information maintained in the victim's web browser can be read, modified, and sent to the attacker.	10.0	More Details
CVE-2023-0016	SAP BPC MS 10.0 - version 810, allows an unauthorized attacker to execute crafted database queries. The exploitation of this issue could lead to SQL injection vulnerability and could allow an attacker to access, modify, and/or delete data from the backend database.	9.9	More Details
CVE-2022-45092	A vulnerability has been identified in SINEC INS (All versions < V1.0 SP2 Update 1). An authenticated remote attacker with access to the Web Based Management (443/tcp) of the affected product, could potentially read and write arbitrary files from and to the device's file system. An attacker might leverage this to trigger remote code execution on the affected component.	9.9	More Details
CVE-2023-0022	SAP BusinessObjects Business Intelligence Analysis edition for OLAP allows an authenticated attacker to inject malicious code that can be executed by the application over the network. On successful exploitation, an attacker can perform operations that may completely compromise the application causing a high impact on the confidentiality, integrity, and availability of the application.	9.9	More Details
CVE-2022-47790	Sourcecodester Dynamic Transaction Queuing System v1.0 is vulnerable to SQL Injection via /queuing/index.php?page=display&id=.	9.8	More Details
CVE-2022-4337	An out-of-bounds read in Organization Specific TLV was found in various versions of OpenvSwitch.	9.8	More Details
CVE-2022-4422	Call Center System developed by Bulutses Information Technologies before version 3.0 has an unauthenticated Sql Injection vulnerability. This has been fixed in the version 3.0	9.8	More Details
CVE-2022-3792	Improper Neutralization of Special Elements used in an SQL Command ('SQL Injection') vulnerability in GullsEye GullsEye terminal operating system allows SQL Injection.This issue affects GullsEye terminal operating system: from unspecified before 5.0.13.	9.8	More Details
CVE-2023-22903	api/views/user.py in LibrePhotos before e19e539 has incorrect access control.	9.8	More Details
CVE-2017-20166	Ecto 2.2.0 lacks a certain protection mechanism associated with the interaction between is_nil and raise.	9.8	More Details

CVE Number	Description	Base Score	Reference
CVE-2022-45875	Improper validation of script alert plugin parameters in Apache DolphinScheduler to avoid remote command execution vulnerability. This issue affects Apache DolphinScheduler version 3.0.1 and prior versions; version 3.1.0 and prior versions. This attack can be performed only by authenticated users which can login to DS.	9.8	More Details
CVE-2022-22088	Memory corruption in Bluetooth HOST due to buffer overflow while parsing the command response received from remote	9.8	More Details
CVE-2022-39073	There is a command injection vulnerability in ZTE MF286R, Due to insufficient validation of the input parameters, an attacker could use the vulnerability to execute arbitrary commands.	9.8	More Details
CVE-2023-22671	Ghidra/RuntimeScripts/Linux/support/launch.sh in NSA Ghidra through 10.2.2 passes user-provided input into eval, leading to command injection when calling analyzeHeadless with untrusted input.	9.8	More Details
CVE-2022-44877	login/index.php in CWP (aka Control Web Panel or CentOS Web Panel) 7 before 0.9.8.1147 allows remote attackers to execute arbitrary OS commands via shell metacharacters in the login parameter.	9.8	More Details
CVE-2022-47544	An issue was discovered in Siren Investigate before 12.1.7. Script variable whitelisting is insufficiently sandboxed.	9.8	More Details
CVE-2022-45995	There is an unauthorized buffer overflow vulnerability in Tenda AX12 v22.03.01.21 _ cn. This vulnerability can cause the web service not to restart or even execute arbitrary code. It is a different vulnerability from CVE-2022-2414.	9.8	More Details
CVE-2022-47523	Zoho ManageEngine Access Manager Plus before 4309, Password Manager Pro before 12210, and PAM360 before 5801 are vulnerable to SQL Injection.	9.8	More Details
CVE-2023-22463	KubePi is a k8s panel. The jwt authentication function of KubePi through version 1.6.2 uses hard-coded Jwtsigkeys, resulting in the same Jwtsigkeys for all online projects. This means that an attacker can forge any jwt token to take over the administrator account of any online project. Furthermore, they may use the administrator to take over the k8s cluster of the target enterprise. `session.go`, the use of hard-coded JwtSigKey, allows an attacker to use this value to forge jwt tokens arbitrarily. The JwtSigKey is confidential and should not be hard-coded in the code. The vulnerability has been fixed in 1.6.3. In the patch, JWT key is specified in app.yml. If the user leaves it blank, a random key will be used. There are no workarounds aside from upgrading.	9.8	More Details
CVE-2022-4338	An integer underflow in Organization Specific TLV was found in various versions of OpenvSwitch.	9.8	More Details
CVE-2022-38490	An issue was discovered in EasyVista 2020.2.125.3 and 2022.1.109.0.03. Some parameters allow SQL injection. Version 2022.1.110.1.02 corrects this issue.	9.6	More Details
CVE-2023-0017	An unauthenticated attacker in SAP NetWeaver AS for Java - version 7.50, due to improper access control, can attach to an open interface and make use of an open naming and directory API to access services which can be used to perform unauthorized operations affecting users and data on the current system. This could allow the attacker to have full read access to user data, make modifications to user data, and make services within the system unavailable.	9.4	More Details
CVE-2022-33219	Memory corruption in Automotive due to integer overflow to buffer overflow while registering a new listener with shared buffer.	9.3	More Details
CVE-2022-46823	A vulnerability has been identified in Mendix SAML (Mendix 8 compatible) (All versions >= V2.3.0 < V2.3.4), Mendix SAML (Mendix 9 compatible, New Track) (All versions >= V3.3.0 < V3.3.9), Mendix SAML (Mendix 9 compatible, Upgrade Track) (All versions >= V3.3.0 < V3.3.8). The affected module is vulnerable to reflected cross-site scripting (XSS) attacks. This could allow an attacker to extract sensitive information by tricking users into accessing a malicious link.	9.3	More Details
CVE-2023-0014	SAP NetWeaver ABAP Server and ABAP Platform - versions SAP_BASIS 700, 701, 702, 710, 711, 730, 731, 740, 750, 751, 752, 753, 754, 755, 756, 757, KERNEL 7.22, 7.53, 7.77, 7.81, 7.85, 7.89, KRNL64UC 7.22, 7.22EXT, 7.53, KRNL64NUC 7.22, 7.22EXT, creates information about system identity in an ambiguous format. This could lead to capture-replay vulnerability and may be exploited by malicious users to obtain illegitimate access to the system.	9.0	More Details

CVE Number	Description	Base Score	Reference
CVE-2023-22457	CKEditor Integration UI adds support for editing wiki pages using CKEditor. Prior to versions 1.64.3,t he `CKEditor.HTMLConverter` document lacked a protection against Cross-Site Request Forgery (CSRF), allowing to execute macros with the rights of the current user. If a privileged user with programming rights was tricked into executing a GET request to this document with certain parameters (e.g., via an image with a corresponding URL embedded in a comment or via a redirect), this would allow arbitrary remote code execution and the attacker could gain rights, access private information or impact the availability of the wiki. The issue has been patched in the CKEditor Integration version 1.64.3. This has also been patched in the version of the CKEditor integration that is bundled starting with XWiki 14.6 RC1. There are no known workarounds for this other than upgrading the CKEditor integration to a fixed version.	9.0	More Details

OTHER VULNERABILITIES

CVE Number	Description	Base Score	Reference
CVE-2023-21744	Microsoft SharePoint Server Remote Code Execution Vulnerability	8.8	More Details
CVE-2022-43519	Multiple vulnerabilities in the web-based management interface of Aruba EdgeConnect Enterprise Orchestrator could allow an authenticated remote attacker to conduct SQL injection attacks against the Aruba EdgeConnect Enterprise Orchestrator instance. An attacker could exploit these vulnerabilities to obtain and modify sensitive information in the underlying database potentially leading to complete compromise of the Aruba EdgeConnect Enterprise Orchestrator host in Aruba EdgeConnect Enterprise Orchestration Software version(s): Aruba EdgeConnect Enterprise Orchestrator (on-premises), Aruba EdgeConnect Enterprise Orchestrator-as-a-Service, Aruba EdgeConnect Enterprise Orchestrator-SP and Aruba EdgeConnect Enterprise Orchestrator Global Enterprise Tenant Orchestrators - Orchestrator 9.2.1.40179 and below, - Orchestrator 9.1.4.40436 and below, - Orchestrator 9.0.7.40110 and below, - Orchestrator 8.10.23.40015 and below, - Any older branches of Orchestrator not specifically mentioned.	8.8	More Details
CVE-2022-43523	Multiple vulnerabilities in the web-based management interface of Aruba EdgeConnect Enterprise Orchestrator could allow an authenticated remote attacker to conduct SQL injection attacks against the Aruba EdgeConnect Enterprise Orchestrator instance. An attacker could exploit these vulnerabilities to obtain and modify sensitive information in the underlying database potentially leading to complete compromise of the Aruba EdgeConnect Enterprise Orchestrator host in Aruba EdgeConnect Enterprise Orchestration Software version(s): Aruba EdgeConnect Enterprise Orchestrator (on-premises), Aruba EdgeConnect Enterprise Orchestrator-as-a-Service, Aruba EdgeConnect Enterprise Orchestrator-SP and Aruba EdgeConnect Enterprise Orchestrator Global Enterprise Tenant Orchestrators - Orchestrator 9.2.1.40179 and below, - Orchestrator 9.1.4.40436 and below, - Orchestrator 9.0.7.40110 and below, - Orchestrator 8.10.23.40015 and below, - Any older branches of Orchestrator not specifically mentioned.	8.8	More Details
CVE-2022-43522	Multiple vulnerabilities in the web-based management interface of Aruba EdgeConnect Enterprise Orchestrator could allow an authenticated remote attacker to conduct SQL injection attacks against the Aruba EdgeConnect Enterprise Orchestrator instance. An attacker could exploit these vulnerabilities to obtain and modify sensitive information in the underlying database potentially leading to complete compromise of the Aruba EdgeConnect Enterprise Orchestrator host in Aruba EdgeConnect Enterprise Orchestration Software version(s): Aruba EdgeConnect Enterprise Orchestrator (on-premises), Aruba EdgeConnect Enterprise Orchestrator-as-a-Service, Aruba EdgeConnect Enterprise Orchestrator-SP and Aruba EdgeConnect Enterprise Orchestrator Global Enterprise Tenant Orchestrators - Orchestrator 9.2.1.40179 and below, - Orchestrator 9.1.4.40436 and below, - Orchestrator 9.0.7.40110 and below, - Orchestrator 8.10.23.40015 and below, - Any older branches of Orchestrator not specifically mentioned.	8.8	More Details
CVE-2022-3679	The Starter Templates by Kadence WP WordPress plugin before 1.2.17 unserialises the content of an imported file, which could lead to PHP object injection issues when an admin import (intentionally or not) a malicious file and a suitable gadget chain is present on the blog.	8.8	More Details
CVE-2022-3417	The WPtouch WordPress plugin before 4.3.45 unserialises the content of an imported settings file, which could lead to PHP object injections issues when an user import (intentionally or not) a malicious settings file and a suitable gadget chain is present on the blog.	8.8	More Details

CVE Number	Description	Base Score	Reference
CVE-2022-43521	Multiple vulnerabilities in the web-based management interface of Aruba EdgeConnect Enterprise Orchestrator could allow an authenticated remote attacker to conduct SQL injection attacks against the Aruba EdgeConnect Enterprise Orchestrator instance. An attacker could exploit these vulnerabilities to obtain and modify sensitive information in the underlying database potentially leading to complete compromise of the Aruba EdgeConnect Enterprise Orchestrator host in Aruba EdgeConnect Enterprise Orchestration Software version(s): Aruba EdgeConnect Enterprise Orchestrator (on-premises), Aruba EdgeConnect Enterprise Orchestrator-as-a-Service, Aruba EdgeConnect Enterprise Orchestrator-SP and Aruba EdgeConnect Enterprise Orchestrator Global Enterprise Tenant Orchestrators - Orchestrator 9.2.1.40179 and below, - Orchestrator 9.1.4.40436 and below, - Orchestrator 9.0.7.40110 and below, - Orchestrator 8.10.23.40015 and below, - Any older branches of Orchestrator not specifically mentioned.	8.8	More Details
CVE-2022-36930	Zoom Rooms for Windows installers before version 5.13.0 contain a local privilege escalation vulnerability. A local low-privileged user could exploit this vulnerability in an attack chain to escalate their privileges to the SYSTEM user.	8.8	More Details
CVE-2022-43520	Multiple vulnerabilities in the web-based management interface of Aruba EdgeConnect Enterprise Orchestrator could allow an authenticated remote attacker to conduct SQL injection attacks against the Aruba EdgeConnect Enterprise Orchestrator instance. An attacker could exploit these vulnerabilities to obtain and modify sensitive information in the underlying database potentially leading to complete compromise of the Aruba EdgeConnect Enterprise Orchestrator host in Aruba EdgeConnect Enterprise Orchestration Software version(s): Aruba EdgeConnect Enterprise Orchestrator (on-premises), Aruba EdgeConnect Enterprise Orchestrator-as-a-Service, Aruba EdgeConnect Enterprise Orchestrator-SP and Aruba EdgeConnect Enterprise Orchestrator Global Enterprise Tenant Orchestrators - Orchestrator 9.2.1.40179 and below, - Orchestrator 9.1.4.40436 and below, - Orchestrator 9.0.7.40110 and below, - Orchestrator 8.10.23.40015 and below, - Any older branches of Orchestrator not specifically mentioned.	8.8	More Details
CVE-2022-36926	Zoom Rooms for macOS clients before version 5.11.3 contain a local privilege escalation vulnerability. A local low-privileged user could exploit this vulnerability to escalate their privileges to root.	8.8	More Details
CVE-2022-23508	Weave GitOps is a simple open source developer platform for people who want cloud native applications, without needing Kubernetes expertise. A vulnerability in GitOps run could allow a local user or process to alter a Kubernetes cluster's resources. GitOps run has a local S3 bucket which it uses for synchronizing files that are later applied against a Kubernetes cluster. Its endpoint had no security controls to block unauthorized access, therefore allowing local users (and processes) on the same machine to see and alter the bucket content. By leveraging this vulnerability, an attacker could pick a workload of their choosing and inject it into the S3 bucket, which resulted in the successful deployment in the target cluster, without the need to provide any credentials to either the S3 bucket nor the target Kubernetes cluster. There are no known workarounds for this issue, please upgrade. This vulnerability has been fixed by commits 75268c4 and 966823b. Users should upgrade to Weave GitOps version >= v0.12.0 released on 08/12/2022. ### Workarounds There is no workaround for this vulnerability. ### References Disclosed by Paulo Gomes, Senior Software Engineer, Weaveworks. ### For more information If you have any questions or comments about this advisory: - Open an issue in [Weave GitOps repository](https://github.com/weaveworks/weave-gitops) - Email us at [support@weave.works] (mailto:support@weave.works)	8.8	More Details
CVE-2022-43530	Vulnerabilities in the web-based management interface of ClearPass Policy Manager could allow an authenticated remote attacker to conduct SQL injection attacks against the ClearPass Policy Manager instance. An attacker could exploit these vulnerabilities to obtain and modify sensitive information in the underlying database potentially leading to complete compromise of the ClearPass Policy Manager cluster in Aruba ClearPass Policy Manager version(s): ClearPass Policy Manager 6.10.x: 6.10.7 and below and ClearPass Policy Manager 6.9.x: 6.9.12 and below.	8.8	More Details
CVE-2023-21549	Windows SMB Witness Service Elevation of Privilege Vulnerability	8.8	More Details
CVE-2023-0088	The Swifty Page Manager plugin for WordPress is vulnerable to Cross-Site Request Forgery in versions up to, and including, 3.0.1. This is due to missing or incorrect nonce validation on several AJAX actions handling page creation and deletion among other things. This makes it possible for unauthenticated attackers to invoke those functions, via forged request granted they can trick a site administrator into performing an action such as clicking on a link.	8.8	More Details
CVE-2023-21732	Microsoft ODBC Driver Remote Code Execution Vulnerability	8.8	More Details
CVE-2023-21674	Windows Advanced Local Procedure Call (ALPC) Elevation of Privilege Vulnerability	8.8	More Details

CVE Number	Description	Base Score	Reference
CVE-2022-42979	Information disclosure due to an insecure hostname validation in the RYDE application 5.8.43 for Android and iOS allows attackers to take over an account via a deep link.	8.8	More Details
CVE-2023-0048	Code Injection in GitHub repository lirantal/daloradius prior to master-branch.	8.8	More Details
CVE-2023-21681	Microsoft WDAC OLE DB provider for SQL Server Remote Code Execution Vulnerability	8.8	More Details
CVE-2022-44149	The web service on Nexxt Amp300 ARN02304U8 42.103.1.5095 and 80.103.2.5045 devices allows remote OS command execution by placing &telnetd in the JSON host field to the ping feature of the goform/sysTools component. Authentication is required	8.8	More Details
CVE-2022-44535	A vulnerability in the Aruba EdgeConnect Enterprise Orchestrator web-based management interface allows remote low-privileged authenticated users to escalate their privileges to those of an administrative user. A successful exploit could allow an attacker to achieve administrative privilege on the web-management interface leading to complete system compromise in Aruba EdgeConnect Enterprise Orchestration Software version(s): Aruba EdgeConnect Enterprise Orchestrator (on-premises), Aruba EdgeConnect Enterprise Orchestrator-as-a-Service, Aruba EdgeConnect Enterprise Orchestrator-SP and Aruba EdgeConnect Enterprise Orchestrator Global Enterprise Tenant Orchestrators - Orchestrator 9.2.1.40179 and below, - Orchestrator 9.1.4.40436 and below, - Orchestrator 9.0.7.40110 and below, - Orchestrator 8.10.23.40015 and below, - Any older branches of Orchestrator not specifically mentioned.	8.8	More Details
CVE-2022-36927	Zoom Rooms for macOS clients before version 5.11.3 contain a local privilege escalation vulnerability. A local low-privileged user could exploit this vulnerability to escalate their privileges to root.	8.8	More Details
CVE-2022-46610	72crm v9 was discovered to contain an arbitrary file upload vulnerability via the avatar upload function. This vulnerability allows attackers to execute arbitrary code via a crafted PHP file.	8.8	More Details
CVE-2022-43844	IBM Robotic Process Automation for Cloud Pak 20.12 through 21.0.3 is vulnerable to broken access control. A user is not correctly redirected to the platform log out screen when logging out of IBM RPA for Cloud Pak. IBM X-Force ID: 239081.	8.8	More Details
CVE-2023-21742	Microsoft SharePoint Server Remote Code Execution Vulnerability	8.8	More Details
CVE-2023-21676	Windows Lightweight Directory Access Protocol (LDAP) Remote Code Execution Vulnerability	8.8	More Details
CVE-2023-0138	Heap buffer overflow in libphonenumber in Google Chrome prior to 109.0.5414.74 allowed a remote attacker to potentially exploit heap corruption via a crafted HTML page. (Chromium security severity: Low)	8.8	More Details
CVE-2023-0137	Heap buffer overflow in Platform Apps in Google Chrome on Chrome OS prior to 109.0.5414.74 allowed an attacker who convinced a user to install a malicious extension to potentially exploit heap corruption via a crafted HTML page. (Chromium security severity: Medium)	8.8	More Details
CVE-2023-0136	Inappropriate implementation in in Fullscreen API in Google Chrome on Android prior to 109.0.5414.74 allowed a remote attacker to execute incorrect security UI via a crafted HTML page. (Chromium security severity: Medium)	8.8	More Details
CVE-2023-0135	Use after free in Cart in Google Chrome prior to 109.0.5414.74 allowed an attacker who convinced a user to install a malicious extension to potentially exploit heap corruption via database corruption and a crafted HTML page. (Chromium security severity: Medium)	8.8	More Details
CVE-2023-0134	Use after free in Cart in Google Chrome prior to 109.0.5414.74 allowed an attacker who convinced a user to install a malicious extension to potentially exploit heap corruption via database corruption and a crafted HTML page. (Chromium security severity: Medium)	8.8	More Details

CVE Number	Description	Base Score	Reference
CVE-2023-0129	Heap buffer overflow in Network Service in Google Chrome prior to 109.0.5414.74 allowed an attacker who convinced a user to install a malicious extension to potentially exploit heap corruption via a crafted HTML page and specific interactions. (Chromium security severity: High)	8.8	More Details
CVE-2023-0128	Use after free in Overview Mode in Google Chrome on Chrome OS prior to 109.0.5414.74 allowed a remote attacker who convinced a user to engage in specific UI interactions to potentially exploit heap corruption via a crafted HTML page. (Chromium security severity: High)	8.8	More Details
CVE-2022-45052	A Local File Inclusion vulnerability has been found in Axiell Iguana CMS. Due to insufficient neutralisation of user input on the url parameter on the Proxy.type.php endpoint, external users are capable of accessing files on the server.	8.8	More Details
CVE-2022-43531	Vulnerabilities in the web-based management interface of ClearPass Policy Manager could allow an authenticated remote attacker to conduct SQL injection attacks against the ClearPass Policy Manager instance. An attacker could exploit these vulnerabilities to obtain and modify sensitive information in the underlying database potentially leading to complete compromise of the ClearPass Policy Manager cluster in Aruba ClearPass Policy Manager version(s): ClearPass Policy Manager 6.10.x: 6.10.7 and below and ClearPass Policy Manager 6.9.x: 6.9.12 and below.	8.8	More Details
CVE-2022-47083	A PHP Object Injection vulnerability in the unserialize() function Spitfire CMS v1.0.475 allows authenticated attackers to execute arbitrary code via sending crafted requests to the web application.	8.8	More Details
CVE-2022-43524	A vulnerability in the web-based management interface of Aruba EdgeConnect Enterprise Orchestrator could allow an authenticated remote attacker to conduct a stored cross-site scripting (XSS) attack against an administrative user of the interface. A successful exploit allows an attacker to execute arbitrary script code in a victim's browser in the context of the affected interface in Aruba EdgeConnect Enterprise Orchestration Software version(s): Aruba EdgeConnect Enterprise Orchestrator (on-premises), Aruba EdgeConnect Enterprise Orchestrator-as-a-Service, Aruba EdgeConnect Enterprise Orchestrator-SP and Aruba EdgeConnect Enterprise Orchestrator Global Enterprise Tenant Orchestrators - Orchestrator 9.2.1.40179 and below, - Orchestrator 9.1.4.40436 and below, - Orchestrator 9.0.7.40110 and below, - Orchestrator 8.10.23.40015 and below, - Any older branches of Orchestrator not specifically mentioned.	8.7	More Details
CVE-2022-45093	A vulnerability has been identified in SINEC INS (All versions < V1.0 SP2 Update 1). An authenticated remote attacker with access to the Web Based Management (443/tcp) of the affected product as well as with access to the SFTP server of the affected product (22/tcp), could potentially read and write arbitrary files from and to the device's file system. An attacker might leverage this to trigger remote code execution on the affected component.	8.5	More Details
CVE-2022-40517	Memory corruption in core due to stack-based buffer overflow	8.4	More Details
CVE-2022-33300	Memory corruption in Automotive Android OS due to improper input validation.	8.4	More Details
CVE-2022-40520	Memory corruption due to stack-based buffer overflow in Core	8.4	More Details
CVE-2022-2483	The bootloader in the Nokia ASIK AirScale system module (versions 474021A.101 and 474021A.102) loads public keys for firmware verification signature. If an attacker modifies the flash contents to corrupt the keys, secure boot could be permanently disabled on a given device.	8.4	More Details
CVE-2022-40516	Memory corruption in Core due to stack-based buffer overflow.	8.4	More Details
CVE-2022-33274	Memory corruption in android core due to improper validation of array index while returning feature ids after license authentication.	8.4	More Details
CVE-2022-33276	Memory corruption due to buffer copy without checking size of input in modem while receiving WMI_REQUEST_STATS_CMDID command.	8.4	More Details
CVE-2022-2484	The signature check in the Nokia ASIK AirScale system module version 474021A.101 can be bypassed allowing an attacker to run modified firmware. This could result in the execution of a malicious kernel, arbitrary programs, or modified Nokia programs.	8.4	More Details

CVE Number	Description	Base Score	Reference
CVE-2022-2482	A vulnerability exists in Nokia's ASIK AirScale system module (versions 474021A.101 and 474021A.102) that could allow an attacker to place a script on the file system accessible from Linux. A script placed in the appropriate place could allow for arbitrary code execution in the bootloader.	8.4	More Details
CVE-2022-45094	A vulnerability has been identified in SINEC INS (All versions < V1.0 SP2 Update 1). An authenticated remote attacker with access to the Web Based Management (443/tcp) of the affected product, could potentially inject commands into the dhcpd configuration of the affected product. An attacker might leverage this to trigger remote code execution on the affected component.	8.4	More Details
CVE-2022-3929	Communication between the client and the server application of the affected products is partially done using CORBA (Common Object Request Broker Architecture) over TCP/IP. This protocol is not encrypted and allows tracing of internal messages. This issue affects * FOXMAN-UN product: FOXMAN-UN R15B, FOXMAN-UN R15A, FOXMAN-UN R14B, FOXMAN-UN R14A, FOXMAN-UN R11B, FOXMAN-UN R11A, FOXMAN-UN R10C, FOXMAN-UN R9C; * UNEM product: UNEM R15B, UNEM R15A, UNEM R14B, UNEM R14A, UNEM R11B, UNEM R11A, UNEM R10C, UNEM R9C. List of CPEs: * cpe:2.3:a:hitachienergy:foxman-un:R15B:*:*:*:*:*:*:*:* * cpe:2.3:a:hitachienergy:foxman-un:R15A:*:*:*:*:*:*:*:* * cpe:2.3:a:hitachienergy:foxman-un:R14B:*:*:*:*:*:*:*:* * cpe:2.3:a:hitachienergy:foxman-un:R14A:*:*:*:*:*:*:*:* * cpe:2.3:a:hitachienergy:foxman-un:R11B:*:*:*:*:*:*:*:* * cpe:2.3:a:hitachienergy:foxman-un:R11A:*:*:*:*:*:*:*:* * cpe:2.3:a:hitachienergy:foxman-un:R10C:*:*:*:*:*:*:*:* * cpe:2.3:a:hitachienergy:foxman-un:R9C:*:*:*:*:*:*:*:* * cpe:2.3:a:hitachienergy:unem:R15B:*:*:*:*:*:*:*:* * cpe:2.3:a:hitachienergy:unem:R15A:*:*:*:*:*:*:*:* * cpe:2.3:a:hitachienergy:unem:R14B:*:*:*:*:*:*:*:* * cpe:2.3:a:hitachienergy:unem:R14A:*:*:*:*:*:*:*:* * cpe:2.3:a:hitachienergy:unem:R11B:*:*:*:*:*:*:*:* * cpe:2.3:a:hitachienergy:unem:R11A:*:*:*:*:*:*:*:* * cpe:2.3:a:hitachienergy:unem:R10C:*:*:*:*:*:*:*:* * cpe:2.3:a:hitachienergy:unem:R9C:*:*:*:*:*:*:*	8.3	More Details
CVE-2022-38491	An issue was discovered in EasyVista 2020.2.125.3 and 2022.1.109.0.03. Part of the application does not implement protection against brute-force attacks. Version 2022.1.133.0 corrects this issue.	8.2	More Details
CVE-2022-33218	Memory corruption in Automotive due to improper input validation.	8.2	More Details
CVE-2022-33283	Information disclosure due to buffer over-read in WLAN while WLAN frame parsing due to missing frame length check.	8.2	More Details
CVE-2022-43513	A vulnerability has been identified in Automation License Manager V5 (All versions), Automation License Manager V6 (All versions < V6.0 SP9 Upd4), TeleControl Server Basic V3 (All versions < V3.1.2). The affected components allow to rename license files with user chosen input without authentication. This could allow an unauthenticated remote attacker to rename and move files as SYSTEM user.	8.2	More Details
CVE-2022-33255	Information disclosure due to buffer over-read in Bluetooth HOST while processing GetFolderItems and GetItemAttribute Cmds from peer device.	8.2	More Details
CVE-2022-33252	Information disclosure due to buffer over-read in WLAN while handling IBSS beacons frame.	8.2	More Details
CVE-2022-33284	Information disclosure due to buffer over-read in WLAN while parsing BTM action frame.	8.2	More Details
CVE-2022-25746	Memory corruption in kernel due to missing checks when updating the access rights of a memextent mapping.	8.1	More Details
CVE-2023-21543	Windows Layer 2 Tunneling Protocol (L2TP) Remote Code Execution Vulnerability	8.1	More Details
CVE-2023-21679	Windows Layer 2 Tunneling Protocol (L2TP) Remote Code Execution Vulnerability	8.1	More Details
CVE-2023-21548	Windows Secure Socket Tunneling Protocol (SSTP) Remote Code Execution Vulnerability	8.1	More Details

CVE Number	Description	Base Score	Reference
CVE-2023-21555	Windows Layer 2 Tunneling Protocol (L2TP) Remote Code Execution Vulnerability	8.1	More Details
CVE-2023-21546	Windows Layer 2 Tunneling Protocol (L2TP) Remote Code Execution Vulnerability	8.1	More Details
CVE-2023-21556	Windows Layer 2 Tunneling Protocol (L2TP) Remote Code Execution Vulnerability	8.1	More Details
CVE-2022-48217	The tf_remapper_node component 1.1.1 for Robot Operating System (ROS) allows attackers, who control the source code of a different node in the same ROS application, to change a robot's behavior. This occurs because a topic name depends on the attacker-controlled old_tf_topic_name and/or new_tf_topic_name parameter. NOTE: the vendor's position is "it is the responsibility of the programmer to make sure that only known and required parameters are set and unexpected parameters are not."	8.1	More Details
CVE-2022-35401	An authentication bypass vulnerability exists in the get_IFTTTTtoken.cgi functionality of Asus RT-AX82U 3.0.0.4.386_49674-ge182230. A specially-crafted HTTP request can lead to full administrative access to the device. An attacker would need to send a series of HTTP requests to exploit this vulnerability.	8.1	More Details
CVE-2023-21535	Windows Secure Socket Tunneling Protocol (SSTP) Remote Code Execution Vulnerability	8.1	More Details
CVE-2022-43974	MatrixSSL 4.0.4 through 4.5.1 has an integer overflow in matrixSslDecodeTls13. A remote attacker might be able to send a crafted TLS Message to cause a buffer overflow and achieve remote code execution. This is fixed in 4.6.0.	8.1	More Details
CVE-2022-43532	A vulnerability in the web-based management interface of ClearPass Policy Manager could allow an authenticated remote attacker to conduct a stored cross-site scripting (XSS) attack against an administrative user of the interface. A successful exploit allows an attacker to execute arbitrary script code in a victim's browser in the context of the affected interface in Aruba ClearPass Policy Manager version(s): ClearPass Policy Manager 6.10.x: 6.10.7 and below and ClearPass Policy Manager 6.9.x: 6.9.12 and below.	8.0	More Details
CVE-2023-22454	Discourse is an option source discussion platform. Prior to version 2.8.14 on the `stable` branch and version 3.0.0.beta16 on the `beta` and `tests-passed` branches, pending post titles can be used for cross-site scripting attacks. Pending posts can be created by unprivileged users when a category has the "require moderator approval of all new topics" setting set. This vulnerability can lead to a full XSS on sites which have modified or disabled Discourse's default Content Security Policy. A patch is available in versions 2.8.14 and 3.0.0.beta16.	8.0	More Details
CVE-2023-21762	Microsoft Exchange Server Spoofing Vulnerability	8.0	More Details
CVE-2023-21745	Microsoft Exchange Server Spoofing Vulnerability	8.0	More Details
CVE-2022-3927	The affected products store both public and private key that are used to sign and protect Custom Parameter Set (CPS) file from modification. An attacker that manages to exploit this vulnerability will be able to change the CPS file, sign it so that it is trusted as the legitimate CPS file. This issue affects * FOXMAN-UN product: FOXMAN-UN R15B, FOXMAN-UN R15A, FOXMAN-UN R14B, FOXMAN-UN R14A, FOXMAN-UN R11B, FOXMAN-UN R11A, FOXMAN-UN R10C, FOXMAN-UN R9C; * UNEM product: UNEM R15B, UNEM R15A, UNEM R14B, UNEM R14A, UNEM R11B, UNEM R11A, UNEM R10C, UNEM R9C. List of CPEs: * cpe:2.3:a:hitachienergy:foxman-un:R15B:*:*:*:*:*:*:*:* * cpe:2.3:a:hitachienergy:foxman-un:R15A:*:*:*:*:*:*:*:* * cpe:2.3:a:hitachienergy:foxman-un:R14B:*:*:*:*:*:*:*:* * cpe:2.3:a:hitachienergy:foxman-un:R14A:*:*:*:*:*:*:*:* * cpe:2.3:a:hitachienergy:foxman-un:R11B:*:*:*:*:*:*:*:* * cpe:2.3:a:hitachienergy:foxman-un:R11A:*:*:*:*:*:*:*:* * cpe:2.3:a:hitachienergy:foxman-un:R10C:*:*:*:*:*:*:*:* * cpe:2.3:a:hitachienergy:foxman-un:R9C:*:*:*:*:*:*:*:* * cpe:2.3:a:hitachienergy:unem:R15B:*:*:*:*:*:*:*:* * cpe:2.3:a:hitachienergy:unem:R15A:*:*:*:*:*:*:*:* * cpe:2.3:a:hitachienergy:unem:R14B:*:*:*:*:*:*:*:* * cpe:2.3:a:hitachienergy:unem:R14A:*:*:*:*:*:*:*:* * cpe:2.3:a:hitachienergy:unem:R11B:*:*:*:*:*:*:*:* * cpe:2.3:a:hitachienergy:unem:R11A:*:*:*:*:*:*:*:* * cpe:2.3:a:hitachienergy:unem:R10C:*:*:*:*:*:*:*:* * cpe:2.3:a:hitachienergy:unem:R9C:*:*:*:*:*:*:*:*	8.0	More Details

CVE Number	Description	Base Score	Reference
CVE-2023-21763	Microsoft Exchange Server Elevation of Privilege Vulnerability	7.8	More Details
CVE-2022-41613	Bentley Systems MicroStation Connect versions 10.17.0.209 and prior are vulnerable to an Out-of-Bounds Read when when parsing DGN files, which may allow an attacker to crash the product, disclose sensitive information, or execute arbitrary code.	7.8	More Details
CVE-2023-21754	Windows Kernel Elevation of Privilege Vulnerability	7.8	More Details
CVE-2023-21764	Microsoft Exchange Server Elevation of Privilege Vulnerability	7.8	More Details
CVE-2023-21755	Windows Kernel Elevation of Privilege Vulnerability	7.8	More Details
CVE-2022-44939	Efs Software Easy Chat Server Version 3.1 was discovered to contain a DLL hijacking vulnerability via the component TextShaping.dll. This vulnerability allows attackers to execute arbitrary code via a crafted DLL.	7.8	More Details
CVE-2022-40201	Bentley Systems MicroStation Connect versions 10.17.0.209 and prior are vulnerable to a Stack-Based Buffer Overflow when a malformed design (DGN) file is parsed. This may allow an attacker to execute arbitrary code.	7.8	More Details
CVE-2022-3715	A flaw was found in the bash package, where a heap-buffer overflow can occur in valid parameter_transform. This issue may lead to memory problems.	7.8	More Details
CVE-2023-21678	Windows Print Spooler Elevation of Privilege Vulnerability	7.8	More Details
CVE-2022-47654	GPAC MP4box 2.1-DEV-rev593-g007bf61a0 is vulnerable to Buffer Overflow in gf_hevc_read_sps_bs_internal function of media_tools/av_parsers.c:8261	7.8	More Details
CVE-2023-21738	Microsoft Office Visio Remote Code Execution Vulnerability	7.8	More Details
CVE-2023-21737	Microsoft Office Visio Remote Code Execution Vulnerability	7.8	More Details
CVE-2023-21746	Windows NTLM Elevation of Privilege Vulnerability	7.8	More Details
CVE-2023-21736	Microsoft Office Visio Remote Code Execution Vulnerability	7.8	More Details
CVE-2022-4378	A stack overflow flaw was found in the Linux kernel's SYSCTL subsystem in how a user changes certain kernel parameters and variables. This flaw allows a local user to crash or potentially escalate their privileges on the system.	7.8	More Details
CVE-2022-47663	GPAC MP4box 2.1-DEV-rev649-ga8f438d20 is vulnerable to buffer overflow in h263dmx_process filters/reframe_h263.c:609	7.8	More Details
CVE-2023-21735	Microsoft Office Remote Code Execution Vulnerability	7.8	More Details

CVE Number	Description	Base Score	Reference
CVE-2022-47661	GPAC MP4Box 2.1-DEV-rev649-ga8f438d20 is vulnerable to Buffer Overflow via media_tools/av_parsers.c:4988 in gf_media_nalu_add_emulation_bytes	7.8	More Details
CVE-2022-47660	GPAC MP4Box 2.1-DEV-rev644-g5c4df2a67 is has an integer overflow in isomedia/isom_write.c	7.8	More Details
CVE-2022-47659	GPAC MP4box 2.1-DEV-rev644-g5c4df2a67 is vulnerable to Buffer Overflow in gf_bs_read_data	7.8	More Details
CVE-2022-47658	GPAC MP4Box 2.1-DEV-rev644-g5c4df2a67 is vulnerable to buffer overflow in function gf_hevc_read_vps_bs_internal of media_tools/av_parsers.c:8039	7.8	More Details
CVE-2022-47657	GPAC MP4Box 2.1-DEV-rev644-g5c4df2a67 is vulnerable to buffer overflow in function hevc_parse_vps_extension of media_tools/av_parsers.c:7662	7.8	More Details
CVE-2022-47656	GPAC MP4box 2.1-DEV-rev617-g85ce76efd is vulnerable to Buffer Overflow in gf_hevc_read_sps_bs_internal function of media_tools/av_parsers.c:8273	7.8	More Details
CVE-2022-47655	Libde265 1.0.9 is vulnerable to Buffer Overflow in function void put_qpel_fallback<unsigned short>	7.8	More Details
CVE-2022-47653	GPAC MP4box 2.1-DEV-rev593-g007bf61a0 is vulnerable to Buffer Overflow in eac3_update_channels function of media_tools/av_parsers.c:9113	7.8	More Details
CVE-2023-21680	Windows Win32k Elevation of Privilege Vulnerability	7.8	More Details
CVE-2022-47095	GPAC MP4box 2.1-DEV-rev574-g9d5bb184b is vulnerable to Buffer overflow in hevc_parse_vps_extension function of media_tools/av_parsers.c	7.8	More Details
CVE-2022-47094	GPAC MP4box 2.1-DEV-rev574-g9d5bb184b is vulnerable to Null pointer dereference via filters/dmx_m2ts.c:343 in m2tsdmx_declare_pid	7.8	More Details
CVE-2022-47093	GPAC MP4box 2.1-DEV-rev574-g9d5bb184b is vulnerable to heap use-after-free via filters/dmx_m2ts.c:470 in m2tsdmx_declare_pid	7.8	More Details
CVE-2023-21734	Microsoft Office Remote Code Execution Vulnerability	7.8	More Details
CVE-2022-47091	GPAC MP4box 2.1-DEV-rev574-g9d5bb184b is vulnerable to Buffer Overflow in gf_text_process_sub function of filters/load_text.c	7.8	More Details
CVE-2022-47089	GPAC MP4box 2.1-DEV-rev574-g9d5bb184b is vulnerable to Buffer Overflow via gf_vvc_read_sps_bs_internal function of media_tools/av_parsers.c	7.8	More Details
CVE-2022-47088	GPAC MP4box 2.1-DEV-rev574-g9d5bb184b is vulnerable to Buffer Overflow.	7.8	More Details
CVE-2022-47087	GPAC MP4box 2.1-DEV-rev574-g9d5bb184b has a Buffer overflow in gf_vvc_read_pps_bs_internal function of media_tools/av_parsers.c	7.8	More Details

CVE Number	Description	Base Score	Reference
CVE-2023-21730	Microsoft Cryptographic Services Elevation of Privilege Vulnerability	7.8	More Details
CVE-2023-21726	Windows Credential Manager User Interface Elevation of Privilege Vulnerability	7.8	More Details
CVE-2023-21724	Microsoft DWM Core Library Elevation of Privilege Vulnerability	7.8	More Details
CVE-2023-21747	Windows Kernel Elevation of Privilege Vulnerability	7.8	More Details
CVE-2023-21748	Windows Kernel Elevation of Privilege Vulnerability	7.8	More Details
CVE-2023-21749	Windows Kernel Elevation of Privilege Vulnerability	7.8	More Details
CVE-2023-21675	Windows Kernel Elevation of Privilege Vulnerability	7.8	More Details
CVE-2023-21793	3D Builder Remote Code Execution Vulnerability	7.8	More Details
CVE-2022-43535	A vulnerability in the ClearPass OnGuard Windows agent could allow malicious users on a Windows instance to elevate their user privileges. A successful exploit could allow these users to execute arbitrary code with NT AUTHORITY\SYSTEM level privileges on the Windows instance in Aruba ClearPass Policy Manager version(s): ClearPass Policy Manager 6.10.x: 6.10.7 and below and ClearPass Policy Manager 6.9.x: 6.9.12 and below.	7.8	More Details
CVE-2023-21773	Windows Kernel Elevation of Privilege Vulnerability	7.8	More Details
CVE-2023-21774	Windows Kernel Elevation of Privilege Vulnerability	7.8	More Details
CVE-2022-43534	A vulnerability in the ClearPass OnGuard Linux agent could allow malicious users on a Linux instance to elevate their user privileges. A successful exploit could allow these users to execute arbitrary code with root level privileges on the Linux instance in Aruba ClearPass Policy Manager version(s): ClearPass Policy Manager 6.10.x: 6.10.7 and below and ClearPass Policy Manager 6.9.x: 6.9.12 and below.	7.8	More Details
CVE-2023-21780	3D Builder Remote Code Execution Vulnerability	7.8	More Details
CVE-2023-21781	3D Builder Remote Code Execution Vulnerability	7.8	More Details
CVE-2023-21782	3D Builder Remote Code Execution Vulnerability	7.8	More Details
CVE-2023-21783	3D Builder Remote Code Execution Vulnerability	7.8	More Details

CVE Number	Description	Base Score	Reference
CVE-2023-21784	3D Builder Remote Code Execution Vulnerability	7.8	More Details
CVE-2023-21785	3D Builder Remote Code Execution Vulnerability	7.8	More Details
CVE-2023-21786	3D Builder Remote Code Execution Vulnerability	7.8	More Details
CVE-2023-21787	3D Builder Remote Code Execution Vulnerability	7.8	More Details
CVE-2023-21788	3D Builder Remote Code Execution Vulnerability	7.8	More Details
CVE-2023-21537	Microsoft Message Queuing (MSMQ) Elevation of Privilege Vulnerability	7.8	More Details
CVE-2022-36929	The Zoom Rooms Installer for Windows prior to 5.12.6 contains a local privilege escalation vulnerability. A local low-privileged user could exploit this vulnerability during the install process to escalate their privileges to the SYSTEM user.	7.8	More Details
CVE-2023-21524	Windows Local Security Authority (LSA) Elevation of Privilege Vulnerability	7.8	More Details
CVE-2022-47935	A vulnerability has been identified in JT Open (All versions < V11.1.1.0), JT Utilities (All versions < V13.1.1.0), Solid Edge (All versions < V2023). The Jt1001.dll contains a memory corruption vulnerability while parsing specially crafted JT files. An attacker could leverage this vulnerability to execute code in the context of the current process. (ZDI-CAN-19078)	7.8	More Details
CVE-2022-47967	A vulnerability has been identified in Solid Edge (All versions < V2023 MP1). The DOCMGMT.DLL contains a memory corruption vulnerability that could be triggered while parsing files in different file formats such as PAR, ASM, DFT. This could allow an attacker to execute code in the context of the current process.	7.8	More Details
CVE-2022-36443	An issue was discovered in Zebra Enterprise Home Screen 4.1.19. The device allows the administrator to lock some communication channels (wireless and SD card) but it is still possible to use a physical connection (Ethernet cable) without restriction.	7.8	More Details
CVE-2023-21789	3D Builder Remote Code Execution Vulnerability	7.8	More Details
CVE-2023-21790	3D Builder Remote Code Execution Vulnerability	7.8	More Details
CVE-2023-21791	3D Builder Remote Code Execution Vulnerability	7.8	More Details
CVE-2023-21792	3D Builder Remote Code Execution Vulnerability	7.8	More Details
CVE-2023-0049	Out-of-bounds Read in GitHub repository vim/vim prior to 9.0.1143.	7.8	More Details

CVE Number	Description	Base Score	Reference
CVE-2023-21779	Visual Studio Code Remote Code Execution Vulnerability	7.8	More Details
CVE-2023-21765	Windows Print Spooler Elevation of Privilege Vulnerability	7.8	More Details
CVE-2023-0054	Out-of-bounds Write in GitHub repository vim/vim prior to 9.0.1145.	7.8	More Details
CVE-2023-21767	Windows Overlay Filter Elevation of Privilege Vulnerability	7.8	More Details
CVE-2023-0051	Heap-based Buffer Overflow in GitHub repository vim/vim prior to 9.0.1144.	7.8	More Details
CVE-2023-21768	Windows Ancillary Function Driver for WinSock Elevation of Privilege Vulnerability	7.8	More Details
CVE-2023-21541	Windows Task Scheduler Elevation of Privilege Vulnerability	7.8	More Details
CVE-2023-21552	Windows GDI Elevation of Privilege Vulnerability	7.8	More Details
CVE-2023-21772	Windows Kernel Elevation of Privilege Vulnerability	7.8	More Details
CVE-2023-21551	Microsoft Cryptographic Services Elevation of Privilege Vulnerability	7.8	More Details
CVE-2023-21561	Microsoft Cryptographic Services Elevation of Privilege Vulnerability	7.8	More Details
CVE-2022-43533	A vulnerability in the ClearPass OnGuard macOS agent could allow malicious users on a macOS instance to elevate their user privileges. A successful exploit could allow these users to execute arbitrary code with root level privileges on the macOS instance in Aruba ClearPass Policy Manager version(s): ClearPass Policy Manager 6.10.x: 6.10.7 and below and ClearPass Policy Manager 6.9.x: 6.9.12 and below.	7.8	More Details
CVE-2023-21558	Windows Error Reporting Service Elevation of Privilege Vulnerability	7.8	More Details
CVE-2022-38492	An issue was discovered in EasyVista 2020.2.125.3 and 2022.1.109.0.03. One parameter allows SQL injection. Version 2022.1.110.1.02 fixes the vulnerability.	7.7	More Details
CVE-2022-43514	A vulnerability has been identified in Automation License Manager V5 (All versions), Automation License Manager V6 (All versions < V6.0 SP9 Upd4), TeleControl Server Basic V3 (All versions < V3.1.2). The affected component does not correctly validate the root path on folder related operations, allowing to modify files and folders outside the intended root directory. This could allow an unauthenticated remote attacker to execute file operations of files outside of the specified root folder. Chained with CVE-2022-43513 this could allow Remote Code Execution.	7.7	More Details
CVE-2023-22461	The `sanitize-svg` package, a small SVG sanitizer to prevent cross-site scripting attacks, uses a deny-list-pattern to sanitize SVGs to prevent XSS. In doing so, literal `<script>`-tags and on-event handlers were detected in versions prior to 0.4.0. As a result, downstream software that relies on `sanitize-svg` and expects resulting SVGs to be safe, may be vulnerable to cross-site scripting. This vulnerability was addressed in v0.4.0. There are no known workarounds	7.6	More Details

CVE Number	Description	Base Score	Reference
CVE-2022-38105	An information disclosure vulnerability exists in the cm_processREQ_NC opcode of Asus RT-AX82U 3.0.0.4.386_49674-ge182230 router's configuration service. A specially-crafted network packets can lead to a disclosure of sensitive information. An attacker can send a network request to trigger this vulnerability.	7.5	More Details
CVE-2023-22479	KubePi is a modern Kubernetes panel. A session fixation attack allows an attacker to hijack a legitimate user session, versions 1.6.3 and below are susceptible. A patch will be released in version 1.6.4.	7.5	More Details
CVE-2023-22895	The bzip2 crate before 0.4.4 for Rust allow attackers to cause a denial of service via a large file that triggers an integer overflow in mem.rs. NOTE: this is unrelated to the https://crates.io/crates/bzip2-rs product.	7.5	More Details
CVE-2023-21677	Windows Internet Key Exchange (IKE) Extension Denial of Service Vulnerability	7.5	More Details
CVE-2023-21557	Windows Lightweight Directory Access Protocol (LDAP) Denial of Service Vulnerability	7.5	More Details
CVE-2023-22320	OpenAM Web Policy Agent (OpenAM Consortium Edition) provided by OpenAM Consortium parses URLs improperly, leading to a path traversal vulnerability(CWE-22). Furthermore, a crafted URL may be evaluated incorrectly.	7.5	More Details
CVE-2022-46081	In Garmin Connect 4.61, terminating a LiveTrack session wouldn't prevent the LiveTrack API from continued exposure of private personal information. NOTE: this is disputed by the vendor because the LiveTrack API service is not a customer-controlled product.	7.5	More Details
CVE-2022-46449	An issue in MPD (Music Player Daemon) v0.23.10 allows attackers to cause a Denial of Service (DoS) via a crafted input.	7.5	More Details
CVE-2022-46163	Travel support program is a rails app to support the travel support program of openSUSE (TSP). Sensitive user data (bank account details, password Hash) can be extracted via Ransack query injection. Every deployment of travel-support-program below the patched version is affected. The travel-support-program uses the Ransack library to implement search functionality. In its default configuration, Ransack will allow for query conditions based on properties of associated database objects [1]. The `*_start`, `*_end` or `*_cont` search matchers [2] can then be abused to exfiltrate sensitive string values of associated database objects via character-by-character brute-force (A match is indicated by the returned JSON not being empty). A single bank account number can be extracted with <200 requests, a password hash can be extracted with ~1200 requests, all within a few minutes. The problem has been patched in commit d22916275c51500b4004933ff1b0a69bc807b2b7. In order to work around this issue, you can also cherry pick that patch, however it will not work without the Rails 5.0 migration that was done in #150, which in turn had quite a few pull requests it depended on.	7.5	More Details
CVE-2022-4636	Black Box KVM Firmware version 3.4.31307 on models ACR1000A-R-R2, ACR1000A-T-R2, ACR1002A-T, ACR1002A-R, and ACR1020A-T is vulnerable to path traversal, which may allow an attacker to steal user credentials and other sensitive information through local file inclusion.	7.5	More Details
CVE-2022-48251	The AES instructions on the ARMv8 platform do not have an algorithm that is "intrinsically resistant" to side-channel attacks. NOTE: the vendor reportedly offers the position "while power side channel attacks ... are possible, they are not directly caused by or related to the Arm architecture."	7.5	More Details
CVE-2022-33285	Transient DOS due to buffer over-read in WLAN while parsing WLAN CSA action frames.	7.5	More Details
CVE-2022-4379	A use-after-free vulnerability was found in __nfs42_ssc_open() in fs/nfs/nfs4file.c in the Linux kernel. This flaw allows an attacker to conduct a remote denial	7.5	More Details
CVE-2023-21527	Windows iSCSI Service Denial of Service Vulnerability	7.5	More Details

CVE Number	Description	Base Score	Reference
CVE-2022-33286	Transient DOS due to buffer over-read in WLAN while processing 802.11 management frames.	7.5	More Details
CVE-2022-33290	Transient DOS in Bluetooth HOST due to null pointer dereference when a mismatched argument is passed.	7.5	More Details
CVE-2022-33299	Transient DOS due to null pointer dereference in Bluetooth HOST while receiving an attribute protocol PDU with zero length data.	7.5	More Details
CVE-2023-21683	Windows Internet Key Exchange (IKE) Extension Denial of Service Vulnerability	7.5	More Details
CVE-2022-33253	Transient DOS due to buffer over-read in WLAN while parsing corrupted NAN frames.	7.5	More Details
CVE-2023-21728	Windows Netlogon Denial of Service Vulnerability	7.5	More Details
CVE-2021-46867	The HW_KEYMASTER module has a problem in releasing memory.Successful exploitation of this vulnerability may result in out-of-bounds memory access.	7.5	More Details
CVE-2022-40049	SQL injection vulnerability in sourcecodester Theme Park Ticketing System 1.0 allows remote attackers to view sensitive information via the id parameter to the /tpts/manage_user.php page.	7.5	More Details
CVE-2021-46868	The HW_KEYMASTER module has a problem in releasing memory.Successful exploitation of this vulnerability may result in out-of-bounds memory access.	7.5	More Details
CVE-2023-21539	Windows Authentication Remote Code Execution Vulnerability	7.5	More Details
CVE-2022-46761	The system has a vulnerability that may cause dynamic hiding and restoring of app icons.Successful exploitation of this vulnerability may cause malicious hiding of app icons.	7.5	More Details
CVE-2022-46762	The memory management module has a logic bypass vulnerability.Successful exploitation of this vulnerability may affect data confidentiality.	7.5	More Details
CVE-2022-47975	The DUBAI module has a double free vulnerability. Successful exploitation of this vulnerability may affect system availability.	7.5	More Details
CVE-2022-47976	The DMSDP module of the distributed hardware has a vulnerability that may cause imposter control connections.Successful exploitation of this vulnerability may disconnect normal service connections.	7.5	More Details
CVE-2023-21538	.NET Denial of Service Vulnerability	7.5	More Details
CVE-2023-21547	Internet Key Exchange (IKE) Protocol Denial of Service Vulnerability	7.5	More Details
CVE-2022-38393	A denial of service vulnerability exists in the cfg_server cm_processConnDiagPktList opcode of Asus RT-AX82U 3.0.0.4.386_49674-ge182230 router's configuration service. A specially-crafted network packet can lead to denial of service. An attacker can send a malicious packet to trigger this vulnerability.	7.5	More Details

CVE Number	Description	Base Score	Reference
CVE-2023-22626	PgHero before 3.1.0 allows Information Disclosure via EXPLAIN because query results may be present in an error message. (Depending on database user privileges, this may only be information from the database, or may be information from file contents on the database server.)	7.5	More Details
CVE-2022-48216	Uniswap Universal Router before 1.1.0 mishandles reentrancy. This would have allowed theft of funds.	7.5	More Details
CVE-2023-22467	Luxon is a library for working with dates and times in JavaScript. On the 1.x branch prior to 1.38.1, the 2.x branch prior to 2.5.2, and the 3.x branch on 3.2.1, Luxon's `DateTime.fromRFC2822() has quadratic (N^2) complexity on some specific inputs. This causes a noticeable slowdown for inputs with lengths above 10k characters. Users providing untrusted data to this method are therefore vulnerable to (Re)DoS attacks. This issue also appears in Moment as CVE-2022-31129. Versions 1.38.1, 2.5.2, and 3.2.1 contain patches for this issue. As a workaround, limit the length of the input.	7.5	More Details
CVE-2022-43932	Improper neutralization of special elements in output used by a downstream component ('Injection') vulnerability in CGI component in Synology Router Manager (SRM) before 1.2.5-8227-6 and 1.3.1-9346-3 allows remote attackers to read arbitrary files via unspecified vectors.	7.5	More Details
CVE-2023-21757	Windows Layer 2 Tunneling Protocol (L2TP) Denial of Service Vulnerability	7.5	More Details
CVE-2023-21758	Windows Internet Key Exchange (IKE) Extension Denial of Service Vulnerability	7.5	More Details
CVE-2023-22460	go-ipld-prime is an implementation of the InterPlanetary Linked Data (IPLD) spec interfaces, a batteries-included codec implementations of IPLD for CBOR and JSON, and tooling for basic operations on IPLD objects. Encoding data which contains a Bytes kind Node will pass a Bytes token to the JSON encoder which will panic as it doesn't expect to receive Bytes tokens. Such an encode should be treated as an error, as plain JSON should not be able to encode Bytes. This only impacts uses of the `json` codec. `dag-json` is not impacted. Use of `json` as a decoder is not impacted. This issue is fixed in v0.19.0. As a workaround, one may prefer the `dag-json` codec, which has the ability to encode bytes.	7.5	More Details
CVE-2023-21761	Microsoft Exchange Server Information Disclosure Vulnerability	7.5	More Details
CVE-2023-22465	Http4s is a Scala interface for HTTP services. Starting with version 0.1.0 and prior to versions 0.21.34, 0.22.15, 0.23.17, and 1.0.0-M38, the `User-Agent` and `Server` header parsers are susceptible to a fatal error on certain inputs. In http4s, modeled headers are lazily parsed, so this only applies to services that explicitly request these typed headers. Fixes are released in 0.21.34, 0.22.15, 0.23.17, and 1.0.0-M38. As a workaround, use the weakly typed header interface.	7.5	More Details
CVE-2022-25923	Versions of the package exec-local-bin before 1.2.0 are vulnerable to Command Injection via the theProcess() functionality due to improper user-input sanitization.	7.4	More Details
CVE-2022-25926	Versions of the package window-control before 1.4.5 are vulnerable to Command Injection via the sendKeys function, due to improper input sanitization.	7.4	More Details
CVE-2022-25890	All versions of the package wifey are vulnerable to Command Injection via the connect() function due to improper input sanitization.	7.4	More Details
CVE-2022-37933	A potential security vulnerability has been identified in HPE Superdome Flex and Superdome Flex 280 servers. The vulnerability could be exploited to allow local unauthorized data injection. HPE has made the following software updates to resolve the vulnerability in HPE Superdome Flex firmware 3.60.50 and below and Superdome Flex 280 servers firmware 1.40.60 and below.	7.3	More Details
CVE-2014-125060	A vulnerability, which was classified as critical, was found in holdennb CollabCal. Affected is the function handleGet of the file calenderServer.cpp. The manipulation leads to improper authentication. It is possible to launch the attack remotely. The patch is identified as b80f6d1893607c99e5113967592417d0fe310ce6. It is recommended to apply a patch to fix this issue. VDB-217614 is the identifier assigned to this vulnerability.	7.3	More Details

CVE Number	Description	Base Score	Reference
CVE-2022-1101	A vulnerability was found in SourceCodester Royale Event Management System 1.0. It has been rated as critical. This issue affects some unknown processing of the file /royal_event/userregister.php. The manipulation leads to improper authentication. The attack may be initiated remotely. The identifier VDB-195785 was assigned to this vulnerability.	7.3	More Details
CVE-2007-10002	A vulnerability, which was classified as critical, has been found in web-cyradm. Affected by this issue is some unknown functionality of the file auth.inc.php. The manipulation of the argument login/login_password/LANG leads to sql injection. The attack may be launched remotely. The name of the patch is 2bcbead3bdb5f118bf2c38c541eaa73c29dcc90f. It is recommended to apply a patch to fix this issue. The identifier of this vulnerability is VDB-217640.	7.3	More Details
CVE-2022-23509	Weave GitOps is a simple open source developer platform for people who want cloud native applications, without needing Kubernetes expertise. GitOps run has a local S3 bucket which it uses for synchronizing files that are later applied against a Kubernetes cluster. The communication between GitOps Run and the local S3 bucket is not encrypted. This allows privileged users or process to tap the local traffic to gain information permitting access to the s3 bucket. From that point, it would be possible to alter the bucket content, resulting in changes in the Kubernetes cluster's resources. There are no known workaround(s) for this vulnerability. This vulnerability has been fixed by commits ce2bbff and babd915. Users should upgrade to Weave GitOps version >= v0.12.0 released on 08/12/2022.	7.3	More Details
CVE-2018-25069	A vulnerability classified as critical has been found in Netis Netcore Router. This affects an unknown part. The manipulation leads to use of hard-coded password. It is possible to initiate the attack remotely. The identifier VDB-217593 was assigned to this vulnerability.	7.3	More Details
CVE-2022-33265	Memory corruption due to information exposure in Powerline Communication Firmware while sending different MMEs from a single, unassociated device.	7.3	More Details
CVE-2022-44534	A vulnerability in the Aruba EdgeConnect Enterprise Orchestrator web-based management interface allows remote authenticated users to run arbitrary commands on the underlying host. A successful exploit could allow an attacker to execute arbitrary commands as root on the underlying operating system leading to complete system compromise in Aruba EdgeConnect Enterprise Orchestration Software version(s): Aruba EdgeConnect Enterprise Orchestrator (on-premises), Aruba EdgeConnect Enterprise Orchestrator-as-a-Service, Aruba EdgeConnect Enterprise Orchestrator-SP and Aruba EdgeConnect Enterprise Orchestrator Global Enterprise Tenant Orchestrators - Orchestrator 9.2.1.40179 and below, - Orchestrator 9.1.4.40436 and below, - Orchestrator 9.0.7.40110 and below, - Orchestrator 8.10.23.40015 and below, - Any older branches of Orchestrator not specifically mentioned.	7.2	More Details
CVE-2023-0046	Improper Restriction of Names for Files and Other Resources in GitHub repository lirantal/daloradius prior to master-branch.	7.2	More Details
CVE-2022-3416	The WPtouch WordPress plugin before 4.3.45 does not properly validate images to be uploaded, allowing high privilege users such as admin to upload arbitrary files on the server even when they should not be allowed to (for example in multisite setup)	7.2	More Details
CVE-2022-43973	An arbitrary code execution vulnerability exisits in Linksys WRT54GL Wireless-G Broadband Router with firmware <= 4.30.18.006. The Check_TSSI function within the httpd binary uses unvalidated user input in the construction of a system command. An authenticated attacker with administrator privileges can leverage this vulnerability over the network via a malicious POST request to /apply.cgi to execute arbitrary commands on the underlying Linux operating system as root.	7.2	More Details
CVE-2022-43971	An arbitrary code exection vulnerability exists in Linksys WUMC710 Wireless-AC Universal Media Connector with firmware <= 1.0.02 (build3). The do_setNTP function within the httpd binary uses unvalidated user input in the construction of a system command. An authenticated attacker with administrator privileges can leverage this vulnerability over the network via a malicious GET or POST request to /setNTP.cgi to execute arbitrary commands on the underlying Linux operating system as root.	7.2	More Details
CVE-2022-43536	Vulnerabilities in the ClearPass Policy Manager web-based management interface allow remote authenticated users to run arbitrary commands on the underlying host. Successful exploits could allow an attacker to execute arbitrary commands as root on the underlying operating system leading to complete system compromise in Aruba ClearPass Policy Manager version(s): ClearPass Policy Manager 6.10.x: 6.10.7 and below and ClearPass Policy Manager 6.9.x: 6.9.12 and below.	7.2	More Details
CVE-2022-43538	Vulnerabilities in the ClearPass Policy Manager web-based management interface allow remote authenticated users to run arbitrary commands on the underlying host. Successful exploits could allow an attacker to execute arbitrary commands as root on the underlying operating system leading to complete system compromise in Aruba ClearPass Policy Manager version(s): ClearPass Policy Manager 6.10.x: 6.10.7 and below and ClearPass Policy Manager 6.9.x: 6.9.12 and below.	7.2	More Details

CVE Number	Description	Base Score	Reference
CVE-2022-43970	A buffer overflow vulnerability exists in Linksys WRT54GL Wireless-G Broadband Router with firmware <= 4.30.18.006. A stack-based buffer overflow in the Start_EPI function within the httpd binary allows an authenticated attacker with administrator privileges to execute arbitrary commands on the underlying Linux operating system as root. This vulnerablity can be triggered over the network via a malicious POST request to /apply.cgi.	7.2	More Details
CVE-2022-43537	Vulnerabilities in the ClearPass Policy Manager web-based management interface allow remote authenticated users to run arbitrary commands on the underlying host. Successful exploits could allow an attacker to execute arbitrary commands as root on the underlying operating system leading to complete system compromise in Aruba ClearPass Policy Manager version(s): ClearPass Policy Manager 6.10.x: 6.10.7 and below and ClearPass Policy Manager 6.9.x: 6.9.12 and below.	7.2	More Details
CVE-2022-4043	The WP Custom Admin Interface WordPress plugin before 7.29 unserialize user input provided via the settings, which could allow high privilege users such as admin to perform PHP Object Injection when a suitable gadget is present.	7.2	More Details
CVE-2023-21741	Microsoft Office Visio Information Disclosure Vulnerability	7.1	More Details
CVE-2022-47092	GPAC MP4box 2.1-DEV-rev574-g9d5bb184b is contains an Integer overflow vulnerability in gf_hevc_read_sps_bs_internal function of media_tools/av_parsers.c:8316	7.1	More Details
CVE-2022-4294	Norton, Avira, Avast and AVG Antivirus for Windows may be susceptible to a Privilege Escalation vulnerability, which is a type of issue whereby an attacker may attempt to compromise the software application to gain elevated access to resources that are normally protected from an application or user.	7.1	More Details
CVE-2023-21752	Windows Backup Service Elevation of Privilege Vulnerability	7.1	More Details
CVE-2023-21760	Windows Print Spooler Elevation of Privilege Vulnerability	7.1	More Details
CVE-2022-36441	An issue was discovered in Zebra Enterprise Home Screen 4.1.19. The Gboard used by different applications can be used to launch and use several other applications that are restricted by the admin.	7.1	More Details
CVE-2021-40341	DES cipher, which has inadequate encryption strength, is used Hitachi Energy FOXMAN-UN to encrypt user credentials used to access the Network Elements. Successful exploitation allows sensitive information to be decrypted easily. This issue affects * FOXMAN-UN product: FOXMAN-UN R16A, FOXMAN-UN R15B, FOXMAN-UN R15A, FOXMAN-UN R14B, FOXMAN-UN R14A, FOXMAN-UN R11B, FOXMAN-UN R11A, FOXMAN-UN R10C, FOXMAN-UN R9C; * UNEM product: UNEM R16A, UNEM R15B, UNEM R15A, UNEM R14B, UNEM R14A, UNEM R11B, UNEM R11A, UNEM R10C, UNEM R9C. List of CPEs: * cpe:2.3:a:hitachienergy:foxman-un:R16A:*:*:*:*:*:*:*:* * cpe:2.3:a:hitachienergy:foxman-un:R15B:*:*:*:*:*:*:*:* * cpe:2.3:a:hitachienergy:foxman-un:R15A:*:*:*:*:*:*:*:* * cpe:2.3:a:hitachienergy:foxman-un:R14B:*:*:*:*:*:*:*:* * cpe:2.3:a:hitachienergy:foxman-un:R14A:*:*:*:*:*:*:*:* * cpe:2.3:a:hitachienergy:foxman-un:R11B:*:*:*:*:*:*:*:* * cpe:2.3:a:hitachienergy:foxman-un:R11A:*:*:*:*:*:*:*:* * cpe:2.3:a:hitachienergy:foxman-un:R10C:*:*:*:*:*:*:*:* * cpe:2.3:a:hitachienergy:foxman-un:R9C:*:*:*:*:*:*:*:* * cpe:2.3:a:hitachienergy:unem:R16A:*:*:*:*:*:*:*:* * cpe:2.3:a:hitachienergy:unem:R15B:*:*:*:*:*:*:*:* * cpe:2.3:a:hitachienergy:unem:R15A:*:*:*:*:*:*:*:* * cpe:2.3:a:hitachienergy:unem:R14B:*:*:*:*:*:*:*:* * cpe:2.3:a:hitachienergy:unem:R14A:*:*:*:*:*:*:*:* * cpe:2.3:a:hitachienergy:unem:R11B:*:*:*:*:*:*:*:* * cpe:2.3:a:hitachienergy:unem:R11A:*:*:*:*:*:*:*:* * cpe:2.3:a:hitachienergy:unem:R10C:*:*:*:*:*:*:*:* * cpe:2.3:a:hitachienergy:unem:R9C:*:*:*:*:*:*:*:*	7.1	More Details

CVE Number	Description	Base Score	Reference
CVE-2021-40342	In the DES implementation, the affected product versions use a default key for encryption. Successful exploitation allows an attacker to obtain sensitive information and gain access to the network elements that are managed by the affected products versions. This issue affects * FOXMAN-UN product: FOXMAN-UN R16A, FOXMAN-UN R15B, FOXMAN-UN R15A, FOXMAN-UN R14B, FOXMAN-UN R14A, FOXMAN-UN R11B, FOXMAN-UN R11A, FOXMAN-UN R10C, FOXMAN-UN R9C; * UNEM product: UNEM R16A, UNEM R15B, UNEM R15A, UNEM R14B, UNEM R14A, UNEM R11B, UNEM R11A, UNEM R10C, UNEM R9C. List of CPEs: * cpe:2.3:a:hitachienergy:foxman-un:R16A:*:*:*:*:*:*:* * cpe:2.3:a:hitachienergy:foxman-un:R15B:*:*:*:*:*:*:* * cpe:2.3:a:hitachienergy:foxman-un:R15A:*:*:*:*:*:*:* * cpe:2.3:a:hitachienergy:foxman-un:R14B:*:*:*:*:*:*:* * cpe:2.3:a:hitachienergy:foxman-un:R14A:*:*:*:*:*:*:* * cpe:2.3:a:hitachienergy:foxman-un:R11B:*:*:*:*:*:*:* * cpe:2.3:a:hitachienergy:foxman-un:R11A:*:*:*:*:*:*:* * cpe:2.3:a:hitachienergy:foxman-un:R10C:*:*:*:*:*:*:* * cpe:2.3:a:hitachienergy:foxman-un:R9C:*:*:*:*:*:*:* * cpe:2.3:a:hitachienergy:unem:R16A:*:*:*:*:*:*:* * cpe:2.3:a:hitachienergy:unem:R15B:*:*:*:*:*:*:* * cpe:2.3:a:hitachienergy:unem:R15A:*:*:*:*:*:*:* * cpe:2.3:a:hitachienergy:unem:R14B:*:*:*:*:*:*:* * cpe:2.3:a:hitachienergy:unem:R14A:*:*:*:*:*:*:* * cpe:2.3:a:hitachienergy:unem:R11B:*:*:*:*:*:*:* * cpe:2.3:a:hitachienergy:unem:R11A:*:*:*:*:*:*:* * cpe:2.3:a:hitachienergy:unem:R10C:*:*:*:*:*:*:* * cpe:2.3:a:hitachienergy:unem:R9C:*:*:*:*:*:*:*	7.1	More Details
CVE-2023-21750	Windows Kernel Elevation of Privilege Vulnerability	7.1	More Details
CVE-2022-3928	Hardcoded credential is found in affected products' message queue. An attacker that manages to exploit this vulnerability will be able to access data to the internal message queue. This issue affects * FOXMAN-UN product: FOXMAN-UN R15B, FOXMAN-UN R15A, FOXMAN-UN R14B, FOXMAN-UN R14A, FOXMAN-UN R11B, FOXMAN-UN R11A, FOXMAN-UN R10C, FOXMAN-UN R9C; * UNEM product: UNEM R15B, UNEM R15A, UNEM R14B, UNEM R14A, UNEM R11B, UNEM R11A, UNEM R10C, UNEM R9C. List of CPEs: * cpe:2.3:a:hitachienergy:foxman-un:R15B:*:*:*:*:*:*:* * cpe:2.3:a:hitachienergy:foxman-un:R15A:*:*:*:*:*:*:* * cpe:2.3:a:hitachienergy:foxman-un:R14B:*:*:*:*:*:*:* * cpe:2.3:a:hitachienergy:foxman-un:R14A:*:*:*:*:*:*:* * cpe:2.3:a:hitachienergy:foxman-un:R11B:*:*:*:*:*:*:* * cpe:2.3:a:hitachienergy:foxman-un:R11A:*:*:*:*:*:*:* * cpe:2.3:a:hitachienergy:foxman-un:R10C:*:*:*:*:*:*:* * cpe:2.3:a:hitachienergy:foxman-un:R9C:*:*:*:*:*:*:* * cpe:2.3:a:hitachienergy:unem:R15B:*:*:*:*:*:*:* * cpe:2.3:a:hitachienergy:unem:R15A:*:*:*:*:*:*:* * cpe:2.3:a:hitachienergy:unem:R14B:*:*:*:*:*:*:* * cpe:2.3:a:hitachienergy:unem:R14A:*:*:*:*:*:*:* * cpe:2.3:a:hitachienergy:unem:R11B:*:*:*:*:*:*:* * cpe:2.3:a:hitachienergy:unem:R11A:*:*:*:*:*:*:* * cpe:2.3:a:hitachienergy:unem:R10C:*:*:*:*:*:*:* * cpe:2.3:a:hitachienergy:unem:R9C:*:*:*:*:*:*:*	7.1	More Details
CVE-2023-21542	Windows Installer Elevation of Privilege Vulnerability	7.0	More Details
CVE-2023-21531	Azure Service Fabric Container Elevation of Privilege Vulnerability	7.0	More Details
CVE-2023-21532	Windows GDI Elevation of Privilege Vulnerability	7.0	More Details
CVE-2023-21739	Windows Bluetooth Driver Elevation of Privilege Vulnerability	7.0	More Details
CVE-2023-21771	Windows Local Session Manager (LSM) Elevation of Privilege Vulnerability	7.0	More Details
CVE-2023-21733	Windows Bind Filter Driver Elevation of Privilege Vulnerability	7.0	More Details
CVE-2022-37934	A potential security vulnerability has been identified in HPE OfficeConnect 1820, and 1850 switch series. The vulnerability could be remotely exploited to allow remote directory traversal in HPE OfficeConnect 1820 switch series version PT.02.17 and below, HPE OfficeConnect 1850 switch series version PC.01.23 and below, and HPE OfficeConnect 1850 (10G aggregator) switch version PO.01.22 and below.	6.8	More Details
CVE-2022-40519	Information disclosure due to buffer overread in Core	6.8	More Details

CVE Number	Description	Base Score	Reference
CVE-2023-21563	BitLocker Security Feature Bypass Vulnerability	6.8	More Details
CVE-2023-22455	Discourse is an option source discussion platform. Prior to version 2.8.14 on the `stable` branch and version 3.0.0.beta16 on the `beta` and `tests-passed` branches, tag descriptions, which can be updated by moderators, can be used for cross-site scripting attacks. This vulnerability can lead to a full XSS on sites which have modified or disabled Discourse's default Content Security Policy. Versions 2.8.14 and 3.0.0.beta16 contain a patch.	6.8	More Details
CVE-2022-40518	Information disclosure due to buffer overread in Core	6.8	More Details
CVE-2022-4432	A buffer over-read vulnerability was reported in the ThinkPadX13s BIOS PersistenceConfigDxe driver that could allow a local attacker with elevated privileges to cause information disclosure.	6.7	More Details
CVE-2022-4435	A buffer over-read vulnerability was reported in the ThinkPadX13s BIOS LenovoRemoteConfigUpdateDxe driver that could allow a local attacker with elevated privileges to cause information disclosure.	6.7	More Details
CVE-2022-4433	A buffer over-read vulnerability was reported in the ThinkPadX13s BIOS LenovoSetupConfigDxe driver that could allow a local attacker with elevated privileges to cause information disclosure.	6.7	More Details
CVE-2022-25717	Memory corruption in display due to double free while allocating frame buffer memory	6.7	More Details
CVE-2022-39087	In network service, there is a missing permission check. This could lead to local escalation of privilege with System execution privileges needed.	6.7	More Details
CVE-2022-25715	Memory corruption in display driver due to incorrect type casting while accessing the fence structure fields	6.7	More Details
CVE-2022-39086	In network service, there is a missing permission check. This could lead to local escalation of privilege with System execution privileges needed.	6.7	More Details
CVE-2022-25721	Memory corruption in video driver due to type confusion error during video playback	6.7	More Details
CVE-2022-39085	In network service, there is a missing permission check. This could lead to local escalation of privilege with System execution privileges needed.	6.7	More Details
CVE-2022-39084	In network service, there is a missing permission check. This could lead to local escalation of privilege with System execution privileges needed.	6.7	More Details
CVE-2022-39088	In network service, there is a missing permission check. This could lead to local escalation of privilege with System execution privileges needed.	6.7	More Details
CVE-2022-4434	A buffer over-read vulnerability was reported in the ThinkPadX13s BIOS driver that could allow a local attacker with elevated privileges to cause information disclosure.	6.7	More Details
CVE-2022-25716	Memory corruption in Multimedia Framework due to unsafe access to the data members	6.7	More Details

CVE Number	Description	Base Score	Reference
CVE-2022-39083	In network service, there is a missing permission check. This could lead to local escalation of privilege with System execution privileges needed.	6.7	More Details
CVE-2022-39082	In network service, there is a missing permission check. This could lead to local escalation of privilege with System execution privileges needed.	6.7	More Details
CVE-2022-39081	In network service, there is a missing permission check. This could lead to local escalation of privilege with System execution privileges needed.	6.7	More Details
CVE-2023-21560	Windows Boot Manager Security Feature Bypass Vulnerability	6.6	More Details
CVE-2023-22898	workers/extractor.py in Pandora (aka pandora-analysis/pandora) 1.3.0 allows a denial of service when an attacker submits a deeply nested ZIP archive (aka ZIP bomb).	6.5	More Details
CVE-2022-23548	Discourse is an option source discussion platform. Prior to version 2.8.14 on the `stable` branch and version 2.9.0.beta16 on the `beta` and `tests-passed` branches, parsing posts can be susceptible to regular expression denial of service (ReDoS) attacks. This issue is patched in versions 2.8.14 and 2.9.0.beta16. There are no known workarounds.	6.5	More Details
CVE-2022-43972	A null pointer dereference vulnerability exists in Linksys WRT54GL Wireless-G Broadband Router with firmware <= 4.30.18.006. A null pointer dereference in the soap_action function within the upnp binary can be triggered by an unauthenticated attacker via a malicious POST request invoking the AddPortMapping action.	6.5	More Details
CVE-2022-45857	An incorrect user management vulnerability [CWE-286] in the FortiManager version 6.4.6 and below VDOM creation component may allow an attacker to access a FortiGate without a password via newly created VDOMs after the super_admin account is deleted.	6.5	More Details
CVE-2023-0077	Integer overflow or wraparound vulnerability in CGI component in Synology Router Manager (SRM) before 1.2.5-8227-6 and 1.3.1-9346-3 allows remote attackers to overflow buffers via unspecified vectors.	6.5	More Details
CVE-2023-0035	softbus_client_stub in communication subsystem within OpenHarmony-v3.0.5 and prior versions has an authentication bypass vulnerability which allows an "SA relay attack".Local attackers can bypass authentication and attack other SAs with high privilege.	6.5	More Details
CVE-2022-45166	An issue was discovered in Archibus Web Central 2022.03.01.107. A service exposed by the application accepts a set of user-controlled parameters that are used to act on the data returned to the user. It allows a basic user to access data unrelated to their role.	6.5	More Details
CVE-2023-0139	Insufficient validation of untrusted input in Downloads in Google Chrome on Windows prior to 109.0.5414.74 allowed a remote attacker to bypass download restrictions via a crafted HTML page. (Chromium security severity: Low)	6.5	More Details
CVE-2022-47974	The Bluetooth AVRCP module has a vulnerability that can lead to DoS attacks.Successful exploitation of this vulnerability may cause the Bluetooth process to restart.	6.5	More Details
CVE-2023-0133	Inappropriate implementation in in Permission prompts in Google Chrome on Android prior to 109.0.5414.74 allowed a remote attacker to bypass main origin permission delegation via a crafted HTML page. (Chromium security severity: Medium)	6.5	More Details
CVE-2023-0140	Inappropriate implementation in in File System API in Google Chrome on Windows prior to 109.0.5414.74 allowed a remote attacker to bypass file system restrictions via a crafted HTML page. (Chromium security severity: Low)	6.5	More Details
CVE-2023-0132	Inappropriate implementation in in Permission prompts in Google Chrome on Windows prior to 109.0.5414.74 allowed a remote attacker to force acceptance of a permission prompt via a crafted HTML page. (Chromium security severity: Medium)	6.5	More Details
CVE-2023-0131	Inappropriate implementation in in iframe Sandbox in Google Chrome prior to 109.0.5414.74 allowed a remote attacker to bypass file download restrictions via a crafted HTML page. (Chromium security severity: Medium)	6.5	More Details

CVE Number	Description	Base Score	Reference
CVE-2022-46258	An incorrect authorization vulnerability was identified in GitHub Enterprise Server that allowed a repository-scoped token with read/write access to modify Action Workflow files without a Workflow scope. The Create or Update file contents API should enforce workflow scope. This vulnerability affected all versions of GitHub Enterprise Server prior to version 3.7 and was fixed in versions 3.3.16, 3.4.11, 3.5.8, and 3.6.4. This vulnerability was reported via the GitHub Bug Bounty program.	6.5	More Details
CVE-2023-0130	Inappropriate implementation in in Fullscreen API in Google Chrome on Android prior to 109.0.5414.74 allowed a remote attacker to spoof the contents of the Omnibox (URL bar) via a crafted HTML page. (Chromium security severity: Medium)	6.5	More Details
CVE-2022-45165	An issue was discovered in Archibus Web Central 2022.03.01.107. A service exposed by the application accepts a user-controlled parameter that is used to create an SQL query. It causes this service to be prone to SQL injection.	6.5	More Details
CVE-2023-0036	platform_callback_stub in misc subsystem within OpenHarmony-v3.0.5 and prior versions has an authentication bypass vulnerability which allows an "SA relay attack".Local attackers can bypass authentication and attack other SAs with high privilege.	6.5	More Details
CVE-2022-4382	A use-after-free flaw caused by a race among the superblock operations in the gadgetfs Linux driver was found. It could be triggered by yanking out a device that is running the gadgetfs side.	6.4	More Details
CVE-2023-0012	In SAP Host Agent (Windows) - versions 7.21, 7.22, an attacker who gains local membership to SAP_LocalAdmin could be able to replace executables with a malicious file that will be started under a privileged account. Note that by default all user members of SAP_LocaAdmin are denied the ability to logon locally by security policy so that this can only occur if the system has already been compromised.	6.4	More Details
CVE-2022-43920	IBM Sterling B2B Integrator Standard Edition 6.0.0.0 through 6.1.2.1 could allow an authenticated user to gain privileges in a different group due to an access control vulnerability in the Sftp server adapter. IBM X-Force ID: 241362.	6.3	More Details
CVE-2021-4300	A vulnerability has been found in ghostlander Halcyon and classified as critical. Affected by this vulnerability is the function CBlock::AddToBlockIndex of the file src/main.cpp of the component Block Verification. The manipulation leads to improper access controls. The attack can be launched remotely. Upgrading to version 1.1.1.0-hal is able to address this issue. The identifier of the patch is 0675b25ae9cc10b5fdc8ea3a32c642979762d45e. It is recommended to upgrade the affected component. The identifier VDB-217417 was assigned to this vulnerability.	6.3	More Details
CVE-2018-25072	A vulnerability classified as critical has been found in lojban jbovlaste. This affects an unknown part of the file dict/listing.html. The manipulation leads to sql injection. It is possible to initiate the attack remotely. The patch is named 6ff44c2e87b1113eb07d76ea62e1f64193b04d15. It is recommended to apply a patch to fix this issue. The associated identifier of this vulnerability is VDB-217647.	6.3	More Details
CVE-2022-2666	A vulnerability has been found in SourceCodester Loan Management System and classified as critical. This vulnerability affects unknown code of the file login.php. The manipulation of the argument username leads to sql injection. The attack can be initiated remotely. The exploit has been disclosed to the public and may be used. VDB-205618 is the identifier assigned to this vulnerability.	6.3	More Details
CVE-2021-4301	A vulnerability was found in slackero phpwcms up to 1.9.26 and classified as critical. Affected by this issue is some unknown functionality. The manipulation of the argument $phpwcms['db_prepend'] leads to sql injection. The attack may be launched remotely. Upgrading to version 1.9.27 is able to address this issue. The patch is identified as 77dafb6a8cc1015f0777daeb5792f43beef77a9d. It is recommended to upgrade the affected component. VDB-217418 is the identifier assigned to this vulnerability.	6.3	More Details
CVE-2021-4307	A vulnerability was found in Yomguithereal Baobab up to 2.6.0. It has been declared as critical. Affected by this vulnerability is an unknown functionality. The manipulation leads to improperly controlled modification of object prototype attributes ('prototype pollution'). The attack can be launched remotely. Upgrading to version 2.6.1 is able to address this issue. The patch is named c56639532a923d9a1600fb863ec7551b188b5d19. It is recommended to upgrade the affected component. The associated identifier of this vulnerability is VDB-217627.	6.3	More Details
CVE-2017-20164	A vulnerability was found in Symbiote Seed up to 6.0.2. It has been classified as critical. Affected is the function onBeforeSecurityLogin of the file code/extensions/SecurityLoginExtension.php of the component Login. The manipulation of the argument URL leads to open redirect. It is possible to launch the attack remotely. Upgrading to version 6.0.3 is able to address this issue. The patch is identified as b065ebd82da53009d273aa7e989191f701485244. It is recommended to upgrade the affected component. VDB-217626 is the identifier assigned to this vulnerability.	6.3	More Details

CVE Number	Description	Base Score	Reference
CVE-2022-22338	IBM Sterling B2B Integrator Standard Edition 6.0.0.0 through 6.1.2.1 is vulnerable to SQL injection. A remote attacker could send specially crafted SQL statements, which could allow the attacker to view, add, modify or delete information in the back-end database. IBM X-Force ID: 219510.	6.3	More Details
CVE-2023-22475	Canarytokens is an open source tool which helps track activity and actions on your network. A Cross-Site Scripting vulnerability was identified in the history page of triggered Canarytokens prior to sha-fb61290. An attacker who discovers an HTTP-based Canarytoken (a URL) can use this to execute Javascript in the Canarytoken's trigger history page (domain: canarytokens.org) when the history page is later visited by the Canarytoken's creator. This vulnerability could be used to disable or delete the affected Canarytoken, or view its activation history. It might also be used as a stepping stone towards revealing more information about the Canarytoken's creator to the attacker. For example, an attacker could recover the email address tied to the Canarytoken, or place Javascript on the history page that redirect the creator towards an attacker-controlled Canarytoken to show the creator's network location. This vulnerability is similar to CVE-2022-31113, but affected parameters reported differently from the Canarytoken trigger request. An attacker could only act on the discovered Canarytoken. This issue did not expose other Canarytokens or other Canarytoken creators. Canarytokens Docker images sha-fb61290 and later contain a patch for this issue.	6.3	More Details
CVE-2023-21725	Windows Malicious Software Removal Tool Elevation of Privilege Vulnerability	6.3	More Details
CVE-2014-125044	A vulnerability, which was classified as critical, was found in soshtolsus wing-tight. This affects an unknown part of the file index.php. The manipulation of the argument p leads to file inclusion. It is possible to initiate the attack remotely. Upgrading to version 1.0.0 is able to address this issue. The patch is named 567bc33e6ed82b0d0179c9add707ac2b257aeaf2. It is recommended to upgrade the affected component. The associated identifier of this vulnerability is VDB-217515.	6.3	More Details
CVE-2018-25068	A vulnerability has been found in devent globalpom-utils up to 4.5.0 and classified as critical. This vulnerability affects the function createTmpDir of the file globalpomutils-fileresources/src/main/java/com/anrisoftware/globalpom/fileresourcemanager/FileResourceManagerProvider.java. The manipulation leads to insecure temporary file. The attack can be initiated remotely. Upgrading to version 4.5.1 is able to address this issue. The patch is identified as 77a820bac2f68e662ce261ecb050c643bd7ee560. It is recommended to upgrade the affected component. VDB-217570 is the identifier assigned to this vulnerability.	6.3	More Details
CVE-2014-125048	A vulnerability, which was classified as critical, has been found in kassi xingwall. This issue affects some unknown processing of the file app/controllers/oauth.js. The manipulation leads to session fixiation. The patch is named e9f0d509e1408743048e29d9c099d36e0e1f6ae7. It is recommended to apply a patch to fix this issue. The associated identifier of this vulnerability is VDB-217559.	6.3	More Details
CVE-2021-4304	A vulnerability was found in eprintsug ulcc-core. It has been declared as critical. Affected by this vulnerability is an unknown functionality of the file cgi/toolbox/toolbox. The manipulation of the argument password leads to command injection. The attack can be launched remotely. The patch is named 811edaae81eb044891594f00062a828f51b22cb1. It is recommended to apply a patch to fix this issue. The associated identifier of this vulnerability is VDB-217447.	6.3	More Details
CVE-2022-25725	Denial of service in MODEM due to improper pointer handling	6.2	More Details
CVE-2021-46871	tag.ex in Phoenix Phoenix.HTML (aka phoenix_html) before 3.0.4 allows XSS in HEEx class attributes.	6.1	More Details
CVE-2023-22911	An issue was discovered in MediaWiki before 1.35.9, 1.36.x through 1.38.x before 1.38.5, and 1.39.x before 1.39.1. E-Widgets does widget replacement in HTML attributes, which can lead to XSS, because widget authors often do not expect that their widget is executed in an HTML attribute context.	6.1	More Details
CVE-2022-36928	Zoom for Android clients before version 5.13.0 contain a path traversal vulnerability. A third party app could exploit this vulnerability to read and write to the Zoom application data directory.	6.1	More Details
CVE-2022-34330	IBM Sterling B2B Integrator Standard Edition 6.0.0.0 through 6.1.2.1 is vulnerable to cross-site scripting. This vulnerability allows users to embed arbitrary JavaScript code in the Web UI thus altering the intended functionality potentially leading to credentials disclosure within a trusted session. IBM X-Force ID: 229469.	6.1	More Details
CVE-2022-38481	An issue was discovered in Mega HOPEX 15.2.0.6110 before V5CP2. The application is prone to reflected Cross-site Scripting (XSS) in several features.	6.1	More Details

CVE Number	Description	Base Score	Reference
CVE-2022-4310	The Slimstat Analytics WordPress plugin before 4.9.3 does not sanitise and escape the URI when logging requests, which could allow unauthenticated attackers to perform Stored Cross-Site Scripting attacks against logged in admin viewing the logs	6.1	More Details
CVE-2023-0057	Improper Restriction of Rendered UI Layers or Frames in GitHub repository pyload/pyload prior to 0.5.0b3.dev33.	6.1	More Details
CVE-2022-43526	Multiple vulnerabilities within the web-based management interface of Aruba EdgeConnect Enterprise Orchestrator could allow a remote attacker to conduct a reflected cross-site scripting (XSS) attack against a user of the interface. A successful exploit could allow an attacker to execute arbitrary script code in a victim's browser in the context of the affected interface in Aruba EdgeConnect Enterprise Orchestration Software version(s): Aruba EdgeConnect Enterprise Orchestrator (on-premises), Aruba EdgeConnect Enterprise Orchestrator-as-a-Service, Aruba EdgeConnect Enterprise Orchestrator-SP and Aruba EdgeConnect Enterprise Orchestrator Global Enterprise Tenant Orchestrators - Orchestrator 9.2.1.40179 and below, - Orchestrator 9.1.4.40436 and below, - Orchestrator 9.0.7.40110 and below, - Orchestrator 8.10.23.40015 and below, - Any older branches of Orchestrator not specifically mentioned.	6.1	More Details
CVE-2022-4710	The Royal Elementor Addons plugin for WordPress is vulnerable to Reflected Cross-Site Scripting in versions up to, and including, 1.3.59, due to due to insufficient input sanitization and output escaping of the 'wpr_ajax_search_link_target' parameter in the 'data_fetch' function. This makes it possible for unauthenticated attackers to inject arbitrary web scripts in pages that execute if they can successfully trick a user into performing an action such as clicking on a link. This is occurring because 'sanitize_text_field' is insufficient to prevent attribute-based Cross-Site Scripting	6.1	More Details
CVE-2022-44870	A reflected cross-site scripting (XSS) vulnerability in maccms10 v2022.1000.3032 allows attackers to execute arbitrary web scripts or HTML via a crafted payload injected into the Name parameter under the AD Management module.	6.1	More Details
CVE-2022-45051	A reflected XSS vulnerability has been found in Axiell Iguana CMS, allowing an attacker to execute code in a victim's browser. The module parameter on the Service.template.cls endpoint does not properly neutralise user input, resulting in the vulnerability.	6.1	More Details
CVE-2022-45049	A reflected XSS vulnerability has been found in Axiell Iguana CMS, allowing an attacker to execute code in a victim's browser. The url parameter on the novelist.php endpoint does not properly neutralise user input, resulting in the vulnerability.	6.1	More Details
CVE-2022-46456	NASM v2.16 was discovered to contain a global buffer overflow in the component dbgdbg_typevalue at /output/outdbg.c.	6.1	More Details
CVE-2022-43525	Multiple vulnerabilities within the web-based management interface of Aruba EdgeConnect Enterprise Orchestrator could allow a remote attacker to conduct a reflected cross-site scripting (XSS) attack against a user of the interface. A successful exploit could allow an attacker to execute arbitrary script code in a victim's browser in the context of the affected interface in Aruba EdgeConnect Enterprise Orchestration Software version(s): Aruba EdgeConnect Enterprise Orchestrator (on-premises), Aruba EdgeConnect Enterprise Orchestrator-as-a-Service, Aruba EdgeConnect Enterprise Orchestrator-SP and Aruba EdgeConnect Enterprise Orchestrator Global Enterprise Tenant Orchestrators - Orchestrator 9.2.1.40179 and below, - Orchestrator 9.1.4.40436 and below, - Orchestrator 9.0.7.40110 and below, - Orchestrator 8.10.23.40015 and below, - Any older branches of Orchestrator not specifically mentioned.	6.1	More Details
CVE-2022-4325	The Post Status Notifier Lite WordPress plugin before 1.10.1 does not sanitise and escape a parameter before outputting it back in the page, leading to a Reflected Cross-Site Scripting which can be used against high privilege users such as admin.	6.1	More Details
CVE-2021-36603	Cross Site Scripting (XSS) in Tasmota firmware 6.5.0 allows remote attackers to inject JavaScript code via a crafted string in the field "Friendly Name 1".	6.1	More Details
CVE-2022-4368	The WP CSV WordPress plugin through 1.8.0.0 does not sanitize and escape a parameter before outputting it back in the page when importing a CSV, and doe snot have CSRF checks in place as well, leading to a Reflected Cross-Site Scripting.	6.1	More Details
CVE-2022-46603	An issue in Inkdrop v5.4.1 allows attackers to execute arbitrary commands via uploading a crafted markdown file.	6.1	More Details

CVE Number	Description	Base Score	Reference
CVE-2022-4374	The Bg Bible References WordPress plugin through 3.8.14 does not sanitize and escape a parameter before outputting it back in the page, leading to a Reflected Cross-Site Scripting.	6.1	More Details
CVE-2022-45911	An issue was discovered in Zimbra Collaboration (ZCS) 9.0. XSS can occur on the Classic UI login page by injecting arbitrary JavaScript code in the username field. This occurs before the user logs into the system, which means that even if the attacker executes arbitrary JavaScript, they will not get any sensitive information.	6.1	More Details
CVE-2023-0013	The ABAP Keyword Documentation of SAP NetWeaver Application Server - versions 702, 731, 740, 750, 751, 752, 753, 754, 755, 756, 757, for ABAP and ABAP Platform does not sufficiently encode user-controlled inputs, resulting in Cross-Site Scripting (XSS) vulnerability. On successful exploitation an attacker can cause limited impact on confidentiality and integrity of the application.	6.1	More Details
CVE-2022-45913	An issue was discovered in Zimbra Collaboration (ZCS) 9.0. XSS can occur via one of attributes in webmail URLs to execute arbitrary JavaScript code, leading to information disclosure.	6.1	More Details
CVE-2022-43527	Multiple vulnerabilities within the web-based management interface of Aruba EdgeConnect Enterprise Orchestrator could allow a remote attacker to conduct a reflected cross-site scripting (XSS) attack against a user of the interface. A successful exploit could allow an attacker to execute arbitrary script code in a victim's browser in the context of the affected interface in Aruba EdgeConnect Enterprise Orchestration Software version(s): Aruba EdgeConnect Enterprise Orchestrator (on-premises), Aruba EdgeConnect Enterprise Orchestrator-as-a-Service, Aruba EdgeConnect Enterprise Orchestrator-SP and Aruba EdgeConnect Enterprise Orchestrator Global Enterprise Tenant Orchestrators - Orchestrator 9.2.1.40179 and below, - Orchestrator 9.1.4.40436 and below, - Orchestrator 9.0.7.40110 and below, - Orchestrator 8.10.23.40015 and below, - Any older branches of Orchestrator not specifically mentioned.	6.1	More Details
CVE-2022-4301	The Sunshine Photo Cart WordPress plugin before 2.9.15 does not sanitise and escape a parameter before outputting it back in the page, leading to a Reflected Cross-Site Scripting.	6.1	More Details
CVE-2022-25722	Information exposure in DSP services due to improper handling of freeing memory	6.0	More Details
CVE-2022-33266	Memory corruption in Audio due to integer overflow to buffer overflow while music playback of clips like amr,evrc,qcelp with modified content.	5.9	More Details
CVE-2023-22899	Zip4j through 2.11.2, as used in Threema and other products, does not always check the MAC when decrypting a ZIP archive.	5.9	More Details
CVE-2023-22469	Deck is a kanban style organization tool aimed at personal planning and project organization for teams integrated with Nextcloud. When getting the reference preview for Deck cards the user has no access to, unauthorized user could eventually get the cached data of a user that has access. There are currently no known workarounds. It is recommended that the Nextcloud app Deck is upgraded to 1.8.2.	5.8	More Details
CVE-2022-2196	A regression exists in the Linux Kernel within KVM: nVMX that allowed for speculative execution attacks. L2 can carry out Spectre v2 attacks on L1 due to L1 thinking it doesn't need retpolines or IBPB after running L2 due to KVM (L0) advertising eIBRS support to L1. An attacker at L2 with code execution can execute code on an indirect branch on the host machine. We recommend upgrading to Kernel 6.2 or past commit 2e7eab81425a	5.8	More Details
CVE-2022-23549	Discourse is an option source discussion platform. Prior to version 2.8.14 on the `stable` branch and version 2.9.0.beta16 on the `beta` and `tests-passed` branches, users can create posts with raw body longer than the `max_length` site setting by including html comments that are not counted toward the character limit. This issue is patched in versions 2.8.14 and 2.9.0.beta16. There are no known workarounds.	5.7	More Details
CVE-2022-43539	A vulnerability exists in the ClearPass Policy Manager cluster communications that allow for an attacker in a privileged network position to potentially obtain sensitive information. A successful exploit could allow an attacker to retrieve information that allows for unauthorized actions as a privileged user on the ClearPass Policy Manager cluster in Aruba ClearPass Policy Manager version(s): ClearPass Policy Manager 6.10.x: 6.10.7 and below and ClearPass Policy Manager 6.9.x: 6.9.12 and below.	5.7	More Details

CVE Number	Description	Base Score	Reference
CVE-2022-46177	Discourse is an option source discussion platform. Prior to version 2.8.14 on the `stable` branch and version 3.0.0.beta16 on the `beta` and `tests-passed` branches, when a user requests for a password reset link email, then changes their primary email, the old reset email is still valid. When the old reset email is used to reset the password, the Discourse account's primary email would be re-linked to the old email. If the old email address is compromised or has transferred ownership, this leads to an account takeover. This is however mitigated by the SiteSetting `email_token_valid_hours` which is currently 48 hours. Users should upgrade to versions 2.8.14 or 3.0.0.beta15 to receive a patch. As a workaround, lower `email_token_valid_hours ` as needed.	5.7	More Details
CVE-2010-10003	A vulnerability classified as critical was found in gesellix titlelink on Joomla. Affected by this vulnerability is an unknown functionality of the file plugin_content_title.php. The manipulation of the argument phrase leads to sql injection. The patch is named b4604e523853965fa981a4e79aef4b554a535db0. It is recommended to apply a patch to fix this issue. The associated identifier of this vulnerability is VDB-217351.	5.5	More Details
CVE-2023-0162	The CPO Companion plugin for WordPress is vulnerable to Stored Cross-Site Scripting via several of its content type settings parameters in versions up to, and including, 1.0.4 due to insufficient input sanitization and output escaping. This makes it possible for authenticated attackers, with administrator-level permissions and above, to inject arbitrary web scripts in pages that will execute whenever a user accesses an injected page.	5.5	More Details
CVE-2014-125073	A vulnerability was found in mapoor voteapp. It has been rated as critical. Affected by this issue is the function create_poll/do_poll/show_poll/show_refresh of the file app.py. The manipulation leads to sql injection. The patch is identified as b290c21a0d8bcdbd55db860afd3cadec97388e72. It is recommended to apply a patch to fix this issue. VDB-217790 is the identifier assigned to this vulnerability.	5.5	More Details
CVE-2022-39116	In sprd_sysdump driver, there is a possible out of bounds write due to a missing bounds check. This could lead to local denial of service in kernel.	5.5	More Details
CVE-2022-39104	In contacts service, there is a missing permission check. This could lead to local denial of service in Contacts service with no additional execution privileges needed.	5.5	More Details
CVE-2022-44435	In messaging service, there is a missing permission check. This could lead to local denial of service in contacts service with no additional execution privileges needed.	5.5	More Details
CVE-2022-44434	In messaging service, there is a missing permission check. This could lead to local denial of service in contacts service with no additional execution privileges needed.	5.5	More Details
CVE-2022-38684	In contacts service, there is a missing permission check. This could lead to local denial of service in contacts service with no additional execution privileges needed.	5.5	More Details
CVE-2022-35281	IBM Maximo Asset Management 7.6.1.1, 7.6.1.2, 7.6.1.3 and the IBM Maximo Manage 8.3, 8.4 application in IBM Maximo Application Suite are vulnerable to CSV injection. IBM X-Force ID: 2306335.	5.5	More Details
CVE-2022-38683	In contacts service, there is a missing permission check. This could lead to local denial of service in contacts service with no additional execution privileges needed.	5.5	More Details
CVE-2022-38678	In contacts service, there is a missing permission check. This could lead to local denial of service in contacts service with no additional execution privileges needed.	5.5	More Details
CVE-2022-44436	In messaging service, there is a missing permission check. This could lead to local denial of service in contacts service with no additional execution privileges needed.	5.5	More Details
CVE-2022-38682	In contacts service, there is a missing permission check. This could lead to local denial of service in contacts service with no additional execution privileges needed.	5.5	More Details
CVE-2022-36442	An issue was discovered in Zebra Enterprise Home Screen 4.1.19. By using the embedded Google Chrome application, it is possible to install an unauthorized application via a downloaded APK.	5.5	More Details

CVE Number	Description	Base Score	Reference
CVE-2022-44432	In wlan driver, there is a possible missing bounds check. This could lead to local denial of service in wlan services.	5.5	More Details
CVE-2022-44431	In wlan driver, there is a possible missing bounds check. This could lead to local denial of service in wlan services.	5.5	More Details
CVE-2023-21776	Windows Kernel Information Disclosure Vulnerability	5.5	More Details
CVE-2022-44446	In wlan driver, there is a possible missing bounds check. This could lead to local denial of service in wlan services.	5.5	More Details
CVE-2016-15017	A vulnerability has been found in fabarea media_upload on TYPO3 and classified as critical. This vulnerability affects the function getUploadedFileList of the file Classes/Service/UploadFileService.php. The manipulation leads to pathname traversal. Upgrading to version 0.9.0 is able to address this issue. The patch is identified as b25d42a4981072321c1a363311d8ea2a4ac8763a. It is recommended to upgrade the affected component. VDB-217786 is the identifier assigned to this vulnerability.	5.5	More Details
CVE-2022-44440	In wlan driver, there is a possible missing bounds check. This could lead to local denial of service in wlan services.	5.5	More Details
CVE-2015-10034	A vulnerability has been found in j-nowak workout-organizer and classified as critical. This vulnerability affects unknown code. The manipulation leads to sql injection. The patch is identified as 13cd6c3d1210640bfdb39872b2bb3597aa991279. It is recommended to apply a patch to fix this issue. VDB-217714 is the identifier assigned to this vulnerability.	5.5	More Details
CVE-2014-125071	A vulnerability was found in lukehutch Gribbit. It has been classified as problematic. Affected is the function messageReceived of the file src/gribbit/request/HttpRequestHandler.java. The manipulation leads to missing origin validation in websockets. The name of the patch is 620418df247aebda3dd4be1dda10fe229ea505dd. It is recommended to apply a patch to fix this issue. The identifier of this vulnerability is VDB-217716.	5.5	More Details
CVE-2022-44438	In messaging service, there is a missing permission check. This could lead to local denial of service in contacts service with no additional execution privileges needed.	5.5	More Details
CVE-2022-44439	In messaging service, there is a missing permission check. This could lead to local denial of service in contacts service with no additional execution privileges needed.	5.5	More Details
CVE-2022-44429	In wlan driver, there is a possible missing bounds check. This could lead to local denial of service in wlan services.	5.5	More Details
CVE-2022-44428	In wlan driver, there is a possible missing bounds check. This could lead to local denial of service in wlan services.	5.5	More Details
CVE-2022-44427	In wlan driver, there is a possible missing bounds check. This could lead to local denial of service in wlan services.	5.5	More Details
CVE-2022-44426	In wlan driver, there is a possible missing bounds check. This could lead to local denial of service in wlan services.	5.5	More Details
CVE-2022-44437	In messaging service, there is a missing permission check. This could lead to local denial of service in contacts service with no additional execution privileges needed.	5.5	More Details
CVE-2014-125072	A vulnerability classified as critical has been found in CherishSin klattr. This affects an unknown part. The manipulation leads to sql injection. The patch is named f8e4ecfbb83aef577011b0b4aebe96fb6ec557f1. It is recommended to apply a patch to fix this issue. The associated identifier of this vulnerability is VDB-217719.	5.5	More Details

CVE Number	Description	Base Score	Reference
CVE-2022-44441	In wlan driver, there is a possible missing bounds check. This could lead to local denial of service in wlan services.	5.5	More Details
CVE-2022-39118	In sprd_sysdump driver, there is a possible out of bounds write due to a missing bounds check. This could lead to local denial of service in kernel.	5.5	More Details
CVE-2022-44425	In wlan driver, there is a possible missing bounds check. This could lead to local denial of service in wlan services.	5.5	More Details
CVE-2022-44424	In music service, there is a missing permission check. This could lead to local denial of service in contacts service with no additional execution privileges needed.	5.5	More Details
CVE-2022-44423	In music service, there is a missing permission check. This could lead to local denial of service in contacts service with no additional execution privileges needed.	5.5	More Details
CVE-2022-44443	In wlan driver, there is a possible missing bounds check. This could lead to local denial of service in wlan services.	5.5	More Details
CVE-2021-4311	A vulnerability classified as problematic was found in Talend Open Studio for MDM. This vulnerability affects unknown code of the component XML Handler. The manipulation leads to xml external entity reference. The patch is identified as 31d442b9fb1d518128fd18f6e4d54e06c3d67793. It is recommended to apply a patch to fix this issue. VDB-217666 is the identifier assigned to this vulnerability.	5.5	More Details
CVE-2022-44422	In music service, there is a missing permission check. This could lead to local denial of service in contacts service with no additional execution privileges needed.	5.5	More Details
CVE-2022-44430	In wlan driver, there is a possible missing bounds check. This could lead to local denial of service in wlan services.	5.5	More Details
CVE-2022-44444	In wlan driver, there is a possible missing bounds check. This could lead to local denial of service in wlan services.	5.5	More Details
CVE-2022-44445	In wlan driver, there is a possible missing bounds check. This could lead to local denial of service in wlan services.	5.5	More Details
CVE-2015-10035	A vulnerability was found in gperson angular-test-reporter and classified as critical. This issue affects the function getProjectTables/addTest of the file rest-server/data-server.js. The manipulation leads to sql injection. The patch is named a29d8ae121b46ebfa96a55a9106466ab2ef166ae. It is recommended to apply a patch to fix this issue. The associated identifier of this vulnerability is VDB-217715.	5.5	More Details
CVE-2022-44442	In wlan driver, there is a possible missing bounds check, This could lead to local denial of service in wlan services.	5.5	More Details
CVE-2023-0087	The Swifty Page Manager plugin for WordPress is vulnerable to Stored Cross-Site Scripting via the 'spm_plugin_options_page_tree_max_width' parameter in versions up to, and including, 3.0.1 due to insufficient input sanitization and output escaping. This makes it possible for authenticated attackers, with administrator-level permissions and above, to inject arbitrary web scripts in pages that will execute whenever a user accesses an injected page. This only affects multi-site installations and installations where unfiltered_html has been disabled.	5.5	More Details
CVE-2014-125051	A vulnerability was found in himiklab yii2-jqgrid-widget up to 1.0.7. It has been declared as critical. This vulnerability affects the function addSearchOptionsRecursively of the file JqGridAction.php. The manipulation leads to sql injection. Upgrading to version 1.0.8 is able to address this issue. The name of the patch is a117e0f2df729e3ff726968794d9a5ac40e660b9. It is recommended to upgrade the affected component. The identifier of this vulnerability is VDB-217564.	5.5	More Details

CVE Number	Description	Base Score	Reference
CVE-2018-25071	A vulnerability was found in roxlukas LMeve up to 0.1.58. It has been rated as critical. Affected by this issue is the function insert_log of the file wwwroot/ccpwgl/proxy.php. The manipulation of the argument fetch leads to sql injection. Upgrading to version 0.1.59-beta is able to address this issue. The patch is identified as c25ff7fe83a2cda1fcb365b182365adc3ffae332. It is recommended to upgrade the affected component. VDB-217610 is the identifier assigned to this vulnerability.	5.5	More Details
CVE-2014-125058	A vulnerability was found in LearnMeSomeCodes project3 and classified as critical. This issue affects the function search_first_name of the file search.rb. The manipulation leads to sql injection. The patch is named d3efa17ae9f6b2fc25a6bbcf165cefed17c7035e. It is recommended to apply a patch to fix this issue. The associated identifier of this vulnerability is VDB-217607. NOTE: Maintainer is aware of this issue as remarked in the source code.	5.5	More Details
CVE-2018-25070	A vulnerability has been found in polterguy Phosphorus Five up to 8.2 and classified as critical. This vulnerability affects the function csv.Read of the file plugins/extras/p5.mysql/NonQuery.cs of the component CSV Import. The manipulation leads to sql injection. Upgrading to version 8.3 is able to address this issue. The patch is identified as c179a3d0703db55cfe0cb939b89593f2e7a87246. It is recommended to upgrade the affected component. VDB-217606 is the identifier assigned to this vulnerability.	5.5	More Details
CVE-2023-21559	Windows Cryptographic Information Disclosure Vulnerability	5.5	More Details
CVE-2015-10022	A vulnerability was found in IISH nlgis2. It has been declared as critical. Affected by this vulnerability is an unknown functionality of the file scripts/etl/custom_import.pl. The manipulation leads to sql injection. The identifier of the patch is 8bdb6fcf7209584eaf1232437f0f53e735b2b34c. It is recommended to apply a patch to fix this issue. The identifier VDB-217609 was assigned to this vulnerability.	5.5	More Details
CVE-2015-10023	A vulnerability classified as critical has been found in Fumon trello-octometric. This affects the function main of the file metrics-ui/server/srv.go. The manipulation of the argument num leads to sql injection. The patch is named a1f1754933fbf21e2221fbc671c81a47de6a04ef. It is recommended to apply a patch to fix this issue. The associated identifier of this vulnerability is VDB-217611.	5.5	More Details
CVE-2015-10017	A vulnerability has been found in HPI-Information-Systems ProLOD and classified as critical. This vulnerability affects unknown code. The manipulation of the argument this leads to sql injection. The name of the patch is 3f710905458d49c77530bd3cbcd8960457566b73. It is recommended to apply a patch to fix this issue. The identifier of this vulnerability is VDB-217552.	5.5	More Details
CVE-2022-4878	A vulnerability classified as critical has been found in JATOS. Affected is the function ZipUtil of the file modules/common/app/utils/common/ZipUtil.java of the component ZIP Handler. The manipulation leads to path traversal. Upgrading to version 3.7.5-alpha is able to address this issue. The name of the patch is 2b42519f309d8164e8811392770ce604cdabb5da. It is recommended to upgrade the affected component. The identifier of this vulnerability is VDB-217548.	5.5	More Details
CVE-2020-36642	A vulnerability was found in trampgeek jobe up to 1.6.x and classified as critical. This issue affects the function run_in_sandbox of the file application/libraries/LanguageTask.php. The manipulation leads to command injection. Upgrading to version 1.7.0 is able to address this issue. The identifier of the patch is 8f43daf50c943b98eaf0c542da901a4a16e85b02. It is recommended to upgrade the affected component. The identifier VDB-217553 was assigned to this vulnerability.	5.5	More Details
CVE-2014-125061	** UNSUPPORTED WHEN ASSIGNED ** A vulnerability was found in peel filebroker and classified as critical. Affected by this issue is the function select_transfer_status_desc of the file lib/common.rb. The manipulation leads to sql injection. The name of the patch is 91097e26a6c84d3208a351afaa52e0f62e5853ef. It is recommended to apply a patch to fix this issue. The identifier of this vulnerability is VDB-217616. NOTE: This vulnerability only affects products that are no longer supported by the maintainer.	5.5	More Details
CVE-2015-10024	A vulnerability classified as critical was found in hoffie larasync. This vulnerability affects unknown code of the file repository/content/file_storage.go. The manipulation leads to path traversal. The name of the patch is 776bad422f4bd4930d09491711246bbeb1be9ba5. It is recommended to apply a patch to fix this issue. The identifier of this vulnerability is VDB-217612.	5.5	More Details
CVE-2022-45935	Usage of temporary files with insecure permissions by the Apache James server allows an attacker with local access to access private user data in transit. Vulnerable components includes the SMTP stack and IMAP APPEND command. This issue affects Apache James server version 3.7.2 and prior versions.	5.5	More Details
CVE-2015-10026	A vulnerability was found in tiredtyrant flairbot. It has been declared as critical. This vulnerability affects unknown code of the file flair.py. The manipulation leads to sql injection. The patch is identified as 5e112b68c6faad1d4699d02c1ebbb7daf48ef8fb. It is recommended to apply a patch to fix this issue. VDB-217618 is the identifier assigned to this vulnerability.	5.5	More Details

CVE Number	Description	Base Score	Reference
CVE-2016-15012	** UNSUPPORTED WHEN ASSIGNED ** A vulnerability was found in forcedotcom SalesforceMobileSDK-Windows up to 4.x. It has been rated as critical. This issue affects the function ComputeCountSql of the file SalesforceSDK/SmartStore/Store/QuerySpec.cs. The manipulation leads to sql injection. Upgrading to version 5.0.0 is able to address this issue. The patch is named 83b3e91e0c1e84873a6d3ca3c5887eb5b4f5a3d8. It is recommended to upgrade the affected component. The associated identifier of this vulnerability is VDB-217619. NOTE: This vulnerability only affects products that are no longer supported by the maintainer.	5.5	More Details
CVE-2022-4880	A vulnerability was found in stakira OpenUtau. It has been classified as critical. This affects the function VoicebankInstaller of the file OpenUtau.Core/Classic/VoicebankInstaller.cs of the component ZIP Archive Handler. The manipulation leads to path traversal. Upgrading to version 0.0.991 is able to address this issue. The identifier of the patch is 849a0a6912aac8b1c28cc32aa1132a3140caff4a. It is recommended to upgrade the affected component. The identifier VDB-217617 was assigned to this vulnerability.	5.5	More Details
CVE-2018-25066	A vulnerability was found in PeterMu nodebatis up to 2.1.x. It has been classified as critical. Affected is an unknown function. The manipulation leads to sql injection. Upgrading to version 2.2.0 is able to address this issue. The patch is identified as 6629ff5b7e3d62ad8319007a54589ec1f62c7c35. It is recommended to upgrade the affected component. VDB-217554 is the identifier assigned to this vulnerability.	5.5	More Details
CVE-2014-125047	A vulnerability classified as critical has been found in tbezman school-store. This affects an unknown part. The manipulation leads to sql injection. The identifier of the patch is 2957fc97054216d3a393f1775efd01ae2b072001. It is recommended to apply a patch to fix this issue. The identifier VDB-217557 was assigned to this vulnerability.	5.5	More Details
CVE-2015-10027	A vulnerability, which was classified as problematic, has been found in hydrian TTRSS-Auth-LDAP. Affected by this issue is some unknown functionality of the component Username Handler. The manipulation leads to ldap injection. Upgrading to version 2.0b1 is able to address this issue. The patch is identified as a7f7a5a82d9202a5c40d606a5c519ba61b224eb8. It is recommended to upgrade the affected component. VDB-217622 is the identifier assigned to this vulnerability.	5.5	More Details
CVE-2020-36640	A vulnerability, which was classified as problematic, was found in bonitasoft bonita-connector-webservice up to 1.3.0. This affects the function TransformerConfigurationException of the file src/main/java/org/bonitasoft/connectors/ws/SecureWSConnector.java. The manipulation leads to xml external entity reference. Upgrading to version 1.3.1 is able to address this issue. The patch is named a12ad691c05af19e9061d7949b6b828ce48815d5. It is recommended to upgrade the affected component. The associated identifier of this vulnerability is VDB-217443.	5.5	More Details
CVE-2018-25067	A vulnerability, which was classified as critical, was found in JoomGallery up to 3.3.3. This affects an unknown part of the file administrator/components/com_joomgallery/views/config/tmpl/default.php of the component Image Sort Handler. The manipulation leads to sql injection. Upgrading to version 3.3.4 is able to address this issue. The identifier of the patch is dc414ee954e849082260f8613e15a1c1e1d354a1. It is recommended to upgrade the affected component. The identifier VDB-217569 was assigned to this vulnerability.	5.5	More Details
CVE-2014-125052	A vulnerability was found in JervenBolleman sparql-identifiers and classified as critical. This issue affects some unknown processing of the file src/main/java/org/identifiers/db/RegistryDao.java. The manipulation leads to sql injection. The patch is named 44bb0db91c064e305b192fc73521d1dfd25bde52. It is recommended to apply a patch to fix this issue. The associated identifier of this vulnerability is VDB-217571.	5.5	More Details
CVE-2019-25097	A vulnerability was found in soerennb eXtplorer up to 2.1.12 and classified as critical. Affected by this issue is some unknown functionality of the component Directory Content Handler. The manipulation leads to path traversal. Upgrading to version 2.1.13 is able to address this issue. The name of the patch is b8fcb888f4ff5e171c16797a4b075c6c6f50bf46. It is recommended to upgrade the affected component. The identifier of this vulnerability is VDB-217436.	5.5	More Details
CVE-2022-43540	A vulnerability exists in the ClearPass OnGuard macOS agent that allows for an attacker with local macOS instance access to potentially obtain sensitive information. A successful exploit could allow an attacker to retrieve information that is of a sensitive nature in Aruba ClearPass Policy Manager version(s): ClearPass Policy Manager 6.10.x: 6.10.7 and below and ClearPass Policy Manager 6.9.x: 6.9.12 and below.	5.5	More Details
CVE-2014-125053	A vulnerability was found in Piwigo-Guest-Book up to 1.3.0. It has been declared as critical. This vulnerability affects unknown code of the file include/guestbook.inc.php of the component Navigation Bar. The manipulation of the argument start leads to sql injection. Upgrading to version 1.3.1 is able to address this issue. The patch is identified as 0cdd1c388edf15089c3a7541cefe7756e560581d. It is recommended to upgrade the affected component. VDB-217582 is the identifier assigned to this vulnerability.	5.5	More Details
CVE-2023-21753	Event Tracing for Windows Information Disclosure Vulnerability	5.5	More Details

CVE Number	Description	Base Score	Reference
CVE-2014-125050	A vulnerability was found in ScottTZhang voter-js and classified as critical. Affected by this issue is some unknown functionality of the file main.js. The manipulation leads to sql injection. The patch is identified as 6317c67a56061aeeaeed3cf9ec665fd9983d8044. It is recommended to apply a patch to fix this issue. VDB-217562 is the identifier assigned to this vulnerability.	5.5	More Details
CVE-2014-125049	** UNSUPPORTED WHEN ASSIGNED ** A vulnerability, which was classified as critical, was found in typcn Blogile. Affected is the function getNav of the file server.js. The manipulation of the argument query leads to sql injection. The name of the patch is cfec31043b562ffefe29fe01af6d3c5ed1bf8f7d. It is recommended to apply a patch to fix this issue. The identifier of this vulnerability is VDB-217560. NOTE: This vulnerability only affects products that are no longer supported by the maintainer.	5.5	More Details
CVE-2020-36641	A vulnerability classified as problematic was found in gturri aXMLRPC up to 1.12.0. This vulnerability affects the function ResponseParser of the file src/main/java/de/timroes/axmlrpc/ResponseParser.java. The manipulation leads to xml external entity reference. Upgrading to version 1.14.0 is able to address this issue. The patch is identified as 456752ebc1ef4c0db980cb5b01a0b3cd0a9e0bae. It is recommended to upgrade the affected component. VDB-217450 is the identifier assigned to this vulnerability.	5.5	More Details
CVE-2014-125040	A vulnerability was found in stevejagodzinski DevNewsAggregator. It has been rated as critical. Affected by this issue is the function getByName of the file php/data_access/RemoteHtmlContentDataAccess.php. The manipulation of the argument name leads to sql injection. The name of the patch is b9de907e7a8c9ca9d75295da675e58c5bf06b172. It is recommended to apply a patch to fix this issue. The identifier of this vulnerability is VDB-217484.	5.5	More Details
CVE-2015-10014	A vulnerability classified as critical has been found in arekk uke. This affects an unknown part of the file lib/uke/finder.rb. The manipulation leads to sql injection. The identifier of the patch is 52fd3b2d0bc16227ef57b7b98a3658bb67c1833f. It is recommended to apply a patch to fix this issue. The identifier VDB-217485 was assigned to this vulnerability.	5.5	More Details
CVE-2014-125041	A vulnerability classified as critical was found in Miccighel PR-CWT. This vulnerability affects unknown code. The manipulation leads to sql injection. The patch is identified as e412127d07004668e5a213932c94807d87067a1f. It is recommended to apply a patch to fix this issue. VDB-217486 is the identifier assigned to this vulnerability.	5.5	More Details
CVE-2019-25099	A vulnerability classified as critical was found in Arthmoor QSF-Portal. This vulnerability affects unknown code of the file index.php. The manipulation of the argument a leads to path traversal. The patch is identified as ea4f61e23ecb83247d174bc2e2cbab521c751a7d. It is recommended to apply a patch to fix this issue. VDB-217558 is the identifier assigned to this vulnerability.	5.5	More Details
CVE-2015-10018	A vulnerability has been found in DBRisinajumi d2files and classified as critical. Affected by this vulnerability is the function actionUpload/actionDownloadFile of the file controllers/D2filesController.php. The manipulation leads to sql injection. Upgrading to version 1.0.0 is able to address this issue. The identifier of the patch is b5767f2ec9d0f3cbfda7f13c84740e2179c90574. It is recommended to upgrade the affected component. The identifier VDB-217561 was assigned to this vulnerability.	5.5	More Details
CVE-2013-10008	A vulnerability was found in sheilazpy eShop. It has been classified as critical. Affected is an unknown function. The manipulation leads to sql injection. The name of the patch is e096c5849c4dc09e1074104531014a62a5413884. It is recommended to apply a patch to fix this issue. The identifier of this vulnerability is VDB-217572.	5.5	More Details
CVE-2014-125062	A vulnerability classified as critical was found in ananich bitstorm. Affected by this vulnerability is an unknown functionality of the file announce.php. The manipulation of the argument event leads to sql injection. The identifier of the patch is ea8da92f94cdb78ee7831e1f7af6258473ab396a. It is recommended to apply a patch to fix this issue. The identifier VDB-217621 was assigned to this vulnerability.	5.5	More Details
CVE-2014-125063	A vulnerability was found in ada-l0velace Bid and classified as critical. This issue affects some unknown processing. The manipulation leads to sql injection. The identifier of the patch is abd71140b8219fa8741d0d8a57ab27d5bfd34222. It is recommended to apply a patch to fix this issue. The identifier VDB-217625 was assigned to this vulnerability.	5.5	More Details
CVE-2022-47086	GPAC MP4Box v2.1-DEV-rev574-g9d5bb184b contains a segmentation violation via the function gf_sm_load_init_swf at scene_manager/swf_parse.c	5.5	More Details
CVE-2020-36645	A vulnerability, which was classified as critical, was found in square squalor. This affects an unknown part. The manipulation leads to sql injection. Upgrading to version v0.0.0 is able to address this issue. The patch is named f6f0a47cc344711042eb0970cb423e6950ba3f93. It is recommended to upgrade the affected component. The associated identifier of this vulnerability is VDB-217623.	5.5	More Details

CVE Number	Description	Base Score	Reference
CVE-2015-10015	A vulnerability, which was classified as critical, has been found in glidernet ogn-live. This issue affects some unknown processing. The manipulation leads to sql injection. The patch is named bc0f19965f760587645583b7624d66a260946e01. It is recommended to apply a patch to fix this issue. The associated identifier of this vulnerability is VDB-217487.	5.5	More Details
CVE-2019-25100	A vulnerability was found in happyman twmap. It has been declared as critical. Affected by this vulnerability is an unknown functionality of the file twmap3/data/ajaxCRUD/pointdata2.php. The manipulation of the argument id leads to sql injection. Upgrading to version v2.9_v4.31 is able to address this issue. The identifier of the patch is babbec79b3fa4efb3bd581ea68af0528d11bba0c. It is recommended to upgrade the affected component. The identifier VDB-217645 was assigned to this vulnerability.	5.5	More Details
CVE-2022-46489	GPAC version 2.1-DEV-rev505-gb9577e6ad-master was discovered to contain a memory leak via the gf_isom_box_parse_ex function at box_funcs.c.	5.5	More Details
CVE-2022-46490	GPAC version 2.1-DEV-rev505-gb9577e6ad-master was discovered to contain a memory leak via the afrt_box_read function at box_code_adobe.c.	5.5	More Details
CVE-2015-10031	A vulnerability classified as critical was found in purpleparrots 491-Project. This vulnerability affects unknown code of the file update.php of the component Highscore Handler. The manipulation leads to sql injection. The name of the patch is a812a5e4cf72f2a635a716086fe1ee2b8fa0b1ab. It is recommended to apply a patch to fix this issue. The identifier of this vulnerability is VDB-217648.	5.5	More Details
CVE-2022-47662	GPAC MP4Box 2.1-DEV-rev649-ga8f438d20 has a segment fault (/stack overflow) due to infinite recursion in Media_GetSample isomedia/media.c:662	5.5	More Details
CVE-2014-125068	A vulnerability was found in saxman maps-js-icoads and classified as critical. This issue affects some unknown processing of the file http-server.js. The manipulation leads to path traversal. The patch is named 34b8b0cce2807b119f4cffda2ac48fc8f427d69a. It is recommended to apply a patch to fix this issue. The associated identifier of this vulnerability is VDB-217643.	5.5	More Details
CVE-2016-15016	A vulnerability was found in mrtnmtth joomla_mod_einsatz_stats up to 0.2. It has been classified as critical. This affects the function getStatsByType of the file helper.php. The manipulation of the argument year leads to sql injection. Upgrading to version 0.3 is able to address this issue. The identifier of the patch is 27c1b443cff45c81d9d7d926a74c76f8b6ffc6cb. It is recommended to upgrade the affected component. The identifier VDB-217653 was assigned to this vulnerability.	5.5	More Details
CVE-2023-21540	Windows Cryptographic Information Disclosure Vulnerability	5.5	More Details
CVE-2014-125045	A vulnerability has been found in meol1 and classified as critical. Affected by this vulnerability is the function GetAnimal of the file opdracht4/index.php. The manipulation of the argument where leads to sql injection. The identifier of the patch is 82441e413f87920d1e8f866e8ef9d7f353a7c583. It is recommended to apply a patch to fix this issue. The identifier VDB-217525 was assigned to this vulnerability.	5.5	More Details
CVE-2022-46457	NASM v2.16 was discovered to contain a segmentation violation in the component ieee_write_file at /output/outieee.c.	5.5	More Details
CVE-2022-23546	In version 2.9.0.beta14 of Discourse, an open-source discussion platform, maliciously embedded urls can leak an admin's digest of recent topics, possibly exposing private information. A patch is available for version 2.9.0.beta15. There are no known workarounds for this issue.	5.5	More Details
CVE-2017-20163	A vulnerability has been found in Red Snapper NView and classified as critical. This vulnerability affects the function mutate of the file src/Session.php. The manipulation of the argument session leads to sql injection. The name of the patch is cbd255f55d476b29e5680f66f48c73ddb3d416a8. It is recommended to apply a patch to fix this issue. The identifier of this vulnerability is VDB-217516.	5.5	More Details
CVE-2022-22371	IBM Sterling B2B Integrator Standard Edition 6.0.0.0 through 6.1.2.1 does not invalidate session after a password change which could allow an authenticated user to impersonate another user on the system. IBM X-Force ID: 221195.	5.5	More Details

CVE Number	Description	Base Score	Reference
CVE-2019-25098	A vulnerability was found in soerennb eXtplorer up to 2.1.12. It has been classified as critical. This affects an unknown part of the file include/archive.php of the component Archive Handler. The manipulation leads to path traversal. Upgrading to version 2.1.13 is able to address this issue. The identifier of the patch is b8fcb888f4ff5e171c16797a4b075c6c6f50bf46. It is recommended to upgrade the affected component. The identifier VDB-217437 was assigned to this vulnerability.	5.5	More Details
CVE-2021-4308	A vulnerability was found in WebPA up to 3.1.1. It has been rated as critical. This issue affects some unknown processing. The manipulation leads to sql injection. Upgrading to version 3.1.2 is able to address this issue. The identifier of the patch is 8836c4f549181e885a68e0e7ca561fdbcbd04bf0. It is recommended to upgrade the affected component. The identifier VDB-217637 was assigned to this vulnerability.	5.5	More Details
CVE-2014-125067	A vulnerability classified as critical was found in corincerami curiosity. Affected by this vulnerability is an unknown functionality of the file app/controllers/image_controller.rb. The manipulation of the argument sol leads to sql injection. The patch is named d64fddd74ca72714e73f4efe24259ca05c8190eb. It is recommended to apply a patch to fix this issue. The associated identifier of this vulnerability is VDB-217639.	5.5	More Details
CVE-2013-10009	A vulnerability was found in DrAzraelTod pyChao and classified as critical. Affected by this issue is the function klauen/lesen of the file mod_fun/__init__.py. The manipulation leads to sql injection. The patch is identified as 9d8adbc07c384ba51c2583ce0819c9abb77dc648. It is recommended to apply a patch to fix this issue. VDB-217634 is the identifier assigned to this vulnerability.	5.5	More Details
CVE-2022-45787	Unproper laxist permissions on the temporary files used by MIME4J TempFileStorageProvider may lead to information disclosure to other local users. This issue affects Apache James MIME4J version 0.8.8 and prior versions. We recommend users to upgrade to MIME4j version 0.8.9 or later.	5.5	More Details
CVE-2014-125065	A vulnerability, which was classified as critical, was found in john5223 bottle-auth. Affected is an unknown function. The manipulation leads to sql injection. The name of the patch is 99cfbcc0c1429096e3479744223ffb4fda276875. It is recommended to apply a patch to fix this issue. The identifier of this vulnerability is VDB-217632.	5.5	More Details
CVE-2015-10029	A vulnerability classified as problematic was found in kelvinmo simplexrd up to 3.1.0. This vulnerability affects unknown code of the file simplexrd/simplexrd.class.php. The manipulation leads to xml external entity reference. Upgrading to version 3.1.1 is able to address this issue. The patch is identified as 4c9f2e028523ed705b555eca2c18c64e71f1a35d. It is recommended to upgrade the affected component. VDB-217630 is the identifier assigned to this vulnerability.	5.5	More Details
CVE-2016-15013	A vulnerability was found in ForumHulp searchresults. It has been rated as critical. Affected by this issue is the function list_keywords of the file event/listener.php. The manipulation of the argument word leads to sql injection. The name of the patch is dd8a312bb285ad9735a8e1da58e9e955837b7322. It is recommended to apply a patch to fix this issue. The identifier of this vulnerability is VDB-217628.	5.5	More Details
CVE-2014-125029	A vulnerability was found in ttskch PaginationServiceProvider up to 0.x. It has been declared as critical. This vulnerability affects unknown code of the file demo/index.php of the component demo. The manipulation of the argument sort/id leads to sql injection. Upgrading to version 1.0.0 is able to address this issue. The patch is identified as 619de478efce17ece1a3b913ab16e40651e1ea7b. It is recommended to upgrade the affected component. VDB-217150 is the identifier assigned to this vulnerability.	5.5	More Details
CVE-2014-125046	A vulnerability, which was classified as critical, was found in Seiji42 cub-scout-tracker. This affects an unknown part of the file databaseAccessFunctions.js. The manipulation leads to sql injection. The patch is named b4bc1a328b1f59437db159f9d136d9ed15707e31. It is recommended to apply a patch to fix this issue. The associated identifier of this vulnerability is VDB-217551.	5.5	More Details
CVE-2023-21550	Windows Cryptographic Information Disclosure Vulnerability	5.5	More Details
CVE-2016-15011	A vulnerability classified as problematic was found in e-Contract dssp up to 1.3.1. Affected by this vulnerability is the function checkSignResponse of the file dssp-client/src/main/java/be/e_contract/dssp/client/SignResponseVerifier.java. The manipulation leads to xml external entity reference. Upgrading to version 1.3.2 is able to address this issue. The identifier of the patch is ec4238349691ec66dd30b416ec6eaab02d722302. It is recommended to upgrade the affected component. The identifier VDB-217549 was assigned to this vulnerability.	5.5	More Details
CVE-2015-10030	A vulnerability has been found in SUKOHI Surpass and classified as critical. This vulnerability affects unknown code of the file src/Sukohi/Surpass/Surpass.php. The manipulation of the argument dir leads to pathname traversal. Upgrading to version 1.0.0 is able to address this issue. The patch is identified as d22337d453a2a14194cdb02bf12cdf9d9f827aa7. It is recommended to upgrade the affected component. VDB-217642 is the identifier assigned to this vulnerability.	5.5	More Details

CVE Number	Description	Base Score	Reference
CVE-2020-36647	A vulnerability classified as critical has been found in YunoHost-Apps transmission_ynh. Affected is an unknown function of the file conf/nginx.conf. The manipulation leads to path traversal. The patch is identified as f136dfd44eda128129e5fd2d850a3a3c600e6a4a. It is recommended to apply a patch to fix this issue. VDB-217638 is the identifier assigned to this vulnerability.	5.5	More Details
CVE-2015-10016	A vulnerability, which was classified as critical, has been found in jeff-kelley opensim-utils. Affected by this issue is the function DatabaseForRegion of the file regionscrits.php. The manipulation of the argument region leads to sql injection. The patch is identified as c29e5c729a833a29dbf5b1e505a0553fe154575e. It is recommended to apply a patch to fix this issue. VDB-217550 is the identifier assigned to this vulnerability.	5.5	More Details
CVE-2020-36648	A vulnerability, which was classified as critical, was found in pouetnet pouet 2.0. This affects an unknown part. The manipulation of the argument howmany leads to sql injection. The identifier of the patch is 11d615931352066fb2f6dcb07428277c2cd99baf. It is recommended to apply a patch to fix this issue. The identifier VDB-217641 was assigned to this vulnerability.	5.5	More Details
CVE-2023-0086	The JetWidgets for Elementor plugin for WordPress is vulnerable to Cross-Site Request Forgery in versions up to, and including, 1.0.12. This is due to missing nonce validation on the save() function. This makes it possible for unauthenticated attackers to to modify the plugin's settings via a forged request granted they can trick a site administrator into performing an action such as clicking on a link. This can be used to enable SVG uploads that could make Cross-Site Scripting possible.	5.4	More Details
CVE-2022-39072	There is a SQL injection vulnerability in Some ZTE Mobile Internet products. Due to insufficient validation of the input parameters of the SNTP interface, an authenticated attacker could use the vulnerability to execute stored XSS attacks.	5.4	More Details
CVE-2021-32828	The Nuxeo Platform is an open source content management platform for building business applications. In version 11.5.109, the `oauth2` REST API is vulnerable to Reflected Cross-Site Scripting (XSS). This XSS can be escalated to Remote Code Execution (RCE) by levering the automation API.	5.4	More Details
CVE-2022-4700	The Royal Elementor Addons plugin for WordPress is vulnerable to insufficient access control in the 'wpr_activate_required_theme' AJAX action in versions up to, and including, 1.3.59. This allows any authenticated user, including those with subscriber-level permissions, to activate the 'royal-elementor-kit' theme. If no such theme is installed doing so can also impact site availability as the site attempts to load a nonexistent theme.	5.4	More Details
CVE-2022-4702	The Royal Elementor Addons plugin for WordPress is vulnerable to insufficient access control in the 'wpr_fix_royal_compatibility' AJAX action in versions up to, and including, 1.3.59. This allows any authenticated user, including those with subscriber-level permissions, to deactivate every plugin on the site unless it is part of an extremely limited hardcoded selection. This also switches the site to the 'royal-elementor-kit' theme, potentially resulting in availability issues.	5.4	More Details
CVE-2022-4704	The Royal Elementor Addons plugin for WordPress is vulnerable to insufficient access control in the 'wpr_import_templates_kit' AJAX action in versions up to, and including, 1.3.59. This allows any authenticated user, including those with subscriber-level permissions, to import preset site configuration templates including images and settings.	5.4	More Details
CVE-2022-4468	The WP Recipe Maker WordPress plugin before 8.6.1 does not validate and escape some of its shortcode attributes before outputting them back in the page, which could allow users with a role as low as contributor to perform Stored Cross-Site Scripting attacks which could be used against high privilege users such as admin.	5.4	More Details
CVE-2023-0110	Cross-site Scripting (XSS) - Stored in GitHub repository usememos/memos prior to 0.10.0.	5.4	More Details
CVE-2021-38928	IBM Sterling B2B Integrator Standard Edition 6.0.0.0 through 6.1.2.1 uses Cross-Origin Resource Sharing (CORS) which could allow an attacker to carry out privileged actions and retrieve sensitive information as the domain name is not being limited to only trusted domains. IBM X-Force ID: 210323.	5.4	More Details
CVE-2022-22352	IBM Sterling B2B Integrator Standard Edition 6.0.0.0 through 6.1.2.1 is vulnerable to cross-site scripting. This vulnerability allows users to embed arbitrary JavaScript code in the Web UI thus altering the intended functionality potentially leading to credentials disclosure within a trusted session. IBM X-Force ID: 220398.	5.4	More Details

CVE Number	Description	Base Score	Reference
CVE-2023-22466	Tokio is a runtime for writing applications with Rust. Starting with version 1.7.0 and prior to versions 1.18.4, 1.20.3, and 1.23.1, when configuring a Windows named pipe server, setting `pipe_mode` will reset `reject_remote_clients` to `false`. If the application has previously configured `reject_remote_clients` to `true`, this effectively undoes the configuration. Remote clients may only access the named pipe if the named pipe's associated path is accessible via a publicly shared folder (SMB). Versions 1.23.1, 1.20.3, and 1.18.4 have been patched. The fix will also be present in all releases starting from version 1.24.0. Named pipes were introduced to Tokio in version 1.7.0, so releases older than 1.7.0 are not affected. As a workaround, ensure that `pipe_mode` is set first after initializing a `ServerOptions`.	5.4	More Details
CVE-2023-0112	Cross-site Scripting (XSS) - Stored in GitHub repository usememos/memos prior to 0.10.0.	5.4	More Details
CVE-2023-0111	Cross-site Scripting (XSS) - Stored in GitHub repository usememos/memos prior to 0.10.0.	5.4	More Details
CVE-2022-46769	An improper neutralization of input during web page generation ('Cross-site Scripting') [CWE-79] vulnerability in Sling App CMS version 1.1.2 and prior may allow an authenticated remote attacker to perform a reflected cross-site scripting (XSS) attack in the site group feature. Upgrade to Apache Sling App CMS >= 1.1.4	5.4	More Details
CVE-2022-4391	The Vision Interactive For WordPress plugin through 1.5.3 does not sanitise and escape some of its settings, which could allow users such as contributor+ to perform Stored Cross-Site Scripting attacks even when the unfiltered_html capability is disallowed.	5.4	More Details
CVE-2022-4392	The iPanorama 360 WordPress Virtual Tour Builder plugin through 1.6.29 does not sanitise and escape some of its settings, which could allow users such as contributor+ to perform Stored Cross-Site Scripting attacks even when the unfiltered_html capability is disallowed.	5.4	More Details
CVE-2022-4393	The ImageLinks Interactive Image Builder for WordPress plugin through 1.5.3 does not sanitise and escape some of its settings, which could allow users such as contributor+ to perform Stored Cross-Site Scripting attacks even when the unfiltered_html capability is disallowed.	5.4	More Details
CVE-2022-4394	The iPages Flipbook For WordPress plugin through 1.4.6 does not sanitise and escape some of its settings, which could allow users such as contributor+ to perform Stored Cross-Site Scripting attacks even when the unfiltered_html capability is disallowed.	5.4	More Details
CVE-2023-0108	Cross-site Scripting (XSS) - Stored in GitHub repository usememos/memos prior to 0.10.0.	5.4	More Details
CVE-2022-4479	The Table of Contents Plus WordPress plugin before 2212 does not validate and escape some of its shortcode attributes before outputting them back in the page, which could allow users with a role as low as contributor to perform Stored Cross-Site Scripting attacks which could be used against high privilege users such as admins.	5.4	More Details
CVE-2022-4491	The WP-Table Reloaded WordPress plugin through 1.9.4 does not validate and escapes some of its shortcode attributes before outputting them back in the page, which could allow users with a role as low as a contributor to perform Stored Cross-Site Scripting attacks, which could be used against high privilege users such as admins.	5.4	More Details
CVE-2022-4497	The Jetpack CRM WordPress plugin before 5.5 does not validate and escape some of its shortcode attributes before outputting them back in the page, which could allow users with a role as low as contributor to perform Stored Cross-Site Scripting attacks which could be used against high privilege users such as admins	5.4	More Details
CVE-2023-0107	Cross-site Scripting (XSS) - Stored in GitHub repository usememos/memos prior to 0.10.0.	5.4	More Details

CVE Number	Description	Base Score	Reference
CVE-2023-22464	ViewVC is a browser interface for CVS and Subversion version control repositories. Versions prior to 1.2.3 and 1.1.30 are vulnerable to cross-site scripting. The impact of this vulnerability is mitigated by the need for an attacker to have commit privileges to a Subversion repository exposed by an otherwise trusted ViewVC instance. The attack vector involves files with unsafe names (names that, when embedded into an HTML stream, would cause the browser to run unwanted code), which themselves can be challenging to create. Users should update to at least version 1.2.3 (if they are using a 1.2.x version of ViewVC) or 1.1.30 (if they are using a 1.1.x version). ViewVC 1.0.x is no longer supported, so users of that release lineage should implement one of the following workarounds. Users can edit their ViewVC EZT view templates to manually HTML-escape changed path "copyfrom paths" during rendering. Locate in your template set's `revision.ezt` file references to those changed paths, and wrap them with `[format "html"]` and `[end]`. For most users, that means that references to `[changes.copy_path]` will become `[format "html"][changes.copy_path][end]`. (This workaround should be reverted after upgrading to a patched version of ViewVC, else "copyfrom path" names will be doubly escaped.)	5.4	More Details
CVE-2023-0106	Cross-site Scripting (XSS) - Stored in GitHub repository usememos/memos prior to 0.10.0.	5.4	More Details
CVE-2023-22909	An issue was discovered in MediaWiki before 1.35.9, 1.36.x through 1.38.x before 1.38.5, and 1.39.x before 1.39.1. SpecialMobileHistory allows remote attackers to cause a denial of service because database queries are slow.	5.3	More Details
CVE-2023-21525	Remote Procedure Call Runtime Denial of Service Vulnerability	5.3	More Details
CVE-2023-22622	WordPress through 6.1.1 depends on unpredictable client visits to cause wp-cron.php execution and the resulting security updates, and the source code describes "the scenario where a site may not receive enough visits to execute scheduled tasks in a timely manner," but neither the installation guide nor the security guide mentions this default behavior, or alerts the user about security risks on installations with very few visits.	5.3	More Details
CVE-2022-0668	JFrog Artifactory prior to 7.37.13 is vulnerable to Authentication Bypass, which can lead to Privilege Escalation when a specially crafted request is sent by an unauthenticated user.	5.3	More Details
CVE-2023-22477	Mercurius is a GraphQL adapter for Fastify. Any users of Mercurius until version 10.5.0 are subjected to a denial of service attack by sending a malformed packet over WebSocket to `/graphql`. This issue was patched in #940. As a workaround, users can disable subscriptions.	5.3	More Details
CVE-2023-0055	Sensitive Cookie in HTTPS Session Without 'Secure' Attribute in GitHub repository pyload/pyload prior to 0.5.0b3.dev32.	5.3	More Details
CVE-2023-22472	Deck is a kanban style organization tool aimed at personal planning and project organization for teams integrated with Nextcloud. It is possible to make a user send any POST request with an arbitrary body given they click on a malicious deep link on a Windows computer. (e.g. in an email, chat link, etc). There are currently no known workarounds. It is recommended that the Nextcloud Desktop client is upgraded to 3.6.2.	5.3	More Details
CVE-2022-30332	In Talend Administration Center 7.3.1.20200219 before TAC-15950, the Forgot Password feature provides different error messages for invalid reset attempts depending on whether the email address is associated with any account. This allows remote attackers to enumerate accounts via a series of requests.	5.3	More Details
CVE-2022-47543	An issue was discovered in Siren Investigate before 12.1.7. There is an ACL bypass on global objects.	5.3	More Details
CVE-2023-0113	A vulnerability was found in Netis Netcore Router up to 2.2.6. It has been declared as problematic. Affected by this vulnerability is an unknown functionality of the file param.file.tgz of the component Backup Handler. The manipulation leads to information disclosure. The attack can be launched remotely. The associated identifier of this vulnerability is VDB-217591.	5.3	More Details
CVE-2023-22453	Discourse is an option source discussion platform. Prior to version 2.8.14 on the `stable` branch and version 3.0.0.beta16 on the `beta` and `tests-passed` branches, the number of times a user posted in an arbitrary topic is exposed to unauthorized users through the `/u/username.json` endpoint. The issue is patched in version 2.8.14 and 3.0.0.beta16. There is no known workaround.	5.3	More Details

CVE Number	Description	Base Score	Reference
CVE-2023-21682	Windows Point-to-Point Protocol (PPP) Information Disclosure Vulnerability	5.3	More Details
CVE-2022-4429	Avira Security for Windows contains an unquoted service path which allows attackers with local administrative privileges to cause a Denial of Service. The issue was fixed with Avira Security version 1.1.78	5.3	More Details
CVE-2023-21743	Microsoft SharePoint Server Security Feature Bypass Vulnerability	5.3	More Details
CVE-2014-125059	A vulnerability, which was classified as problematic, has been found in sternenseemann sternenblog. This issue affects the function blog_index of the file main.c. The manipulation of the argument post_path leads to file inclusion. The attack may be initiated remotely. The complexity of an attack is rather high. The exploitation is known to be difficult. Upgrading to version 0.1.0 is able to address this issue. The identifier of the patch is cf715d911d8ce17969a7926dea651e930c27e71a. It is recommended to upgrade the affected component. The identifier VDB-217613 was assigned to this vulnerability. NOTE: This case is rather theoretical and probably won't happen. Maybe only on obscure Web servers.	5.0	More Details
CVE-2022-46180	Discourse Mermaid (discourse-mermaid-theme-component) allows users of Discourse, open-source forum software, to create graphs using the Mermaid syntax. Users of discourse-mermaid-theme-component version 1.0.0 who can create posts are able to inject arbitrary HTML on that post. The issue has been fixed on the `main` branch of the GitHub repository, with 1.1.0 named as a patched version. Admins can update the theme component through the admin UI. As a workaround, admins can temporarily disable discourse-mermaid-theme-component.	5.0	More Details
CVE-2022-4196	The Multi Step Form WordPress plugin before 1.7.8 does not sanitise and escape some of its form fields, which could allow high privilege users such as admin to perform Stored Cross-Site Scripting attacks even when the unfiltered_html capability is disallowed (for example in multisite setup).	4.8	More Details
CVE-2022-43528	Under certain configurations, an attacker can login to Aruba EdgeConnect Enterprise Orchestrator without supplying a multi-factor authentication code. Successful exploitation allows an attacker to login using only a username and password and successfully bypass MFA requirements in Aruba EdgeConnect Enterprise Orchestration Software version(s): Aruba EdgeConnect Enterprise Orchestrator (on-premises), Aruba EdgeConnect Enterprise Orchestrator-as-a-Service, Aruba EdgeConnect Enterprise Orchestrator-SP and Aruba EdgeConnect Enterprise Orchestrator Global Enterprise Tenant Orchestrators - Orchestrator 9.2.1.40179 and below, - Orchestrator 9.1.4.40436 and below, - Orchestrator 9.0.7.40110 and below, - Orchestrator 8.10.23.40015 and below, - Any older branches of Orchestrator not specifically mentioned.	4.8	More Details
CVE-2022-38489	An issue was discovered in EasyVista 2020.2.125.3 and 2022.1.109.0.03 It is prone to stored Cross-site Scripting (XSS). Version 2022.1.110.1.02 fixes the vulnerably.	4.8	More Details
CVE-2022-3855	The 404 to Start WordPress plugin through 1.6.1 does not sanitise and escape some of its settings, which could allow high privilege users such as admin to perform Stored Cross-Site Scripting attacks even when the unfiltered_html capability is disallowed (for example in multisite setup).	4.8	More Details
CVE-2023-21766	Windows Overlay Filter Information Disclosure Vulnerability	4.7	More Details
CVE-2023-21536	Event Tracing for Windows Information Disclosure Vulnerability	4.7	More Details
CVE-2022-22079	Denial of service while processing fastboot flash command on mmc due to buffer over read	4.6	More Details
CVE-2022-41740	IBM Robotic Process Automation 20.12 through 21.0.6 could allow an attacker with physical access to the system to obtain highly sensitive information from system memory. IBM X-Force ID: 238053.	4.6	More Details

CVE Number	Description	Base Score	Reference
CVE-2022-43529	A vulnerability in the web-based management interface of Aruba EdgeConnect Enterprise Orchestrator could allow an remote attacker to persist a session after a password reset or similar session clearing event. Successful exploitation of this vulnerability could allow an authenticated attacker to remain on the system with the permissions of their current session after the session should be invalidated in Aruba EdgeConnect Enterprise Orchestration Software version(s): Aruba EdgeConnect Enterprise Orchestrator (on-premises), Aruba EdgeConnect Enterprise Orchestrator-as-a-Service, Aruba EdgeConnect Enterprise Orchestrator-SP and Aruba EdgeConnect Enterprise Orchestrator Global Enterprise Tenant Orchestrators - Orchestrator 9.2.1.40179 and below, - Orchestrator 9.1.4.40436 and below, - Orchestrator 9.0.7.40110 and below, - Orchestrator 8.10.23.40015 and below, - Any older branches of Orchestrator not specifically mentioned.	4.6	More Details
CVE-2022-4879	A vulnerability was found in Forged Alliance Forever up to 3746. It has been declared as critical. Affected by this vulnerability is an unknown functionality of the component Vote Handler. The manipulation leads to improper authorization. Upgrading to version 3747 is able to address this issue. The patch is named 6880971bd3d73d942384aff62d53058c206ce644. It is recommended to upgrade the affected component. The associated identifier of this vulnerability is VDB-217555.	4.6	More Details
CVE-2022-38773	Affected devices do not contain an Immutable Root of Trust in Hardware. With this the integrity of the code executed on the device can not be validated during load-time. An attacker with physical access to the device could use this to replace the boot image of the device and execute arbitrary code.	4.6	More Details
CVE-2023-0015	In SAP BusinessObjects Business Intelligence Platform (Web Intelligence user interface) - version 420, some calls return json with wrong content type in the header of the response. As a result, a custom application that calls directly the jsp of Web Intelligence DHTML may be vulnerable to XSS attacks. On successful exploitation an attacker can cause limited impact on confidentiality and integrity of the application.	4.6	More Details
CVE-2023-0023	In SAP Bank Account Management (Manage Banks) application, when a user clicks a smart link to navigate to another app, personal data is shown directly in the URL. They might get captured in log files, bookmarks, and so on disclosing sensitive data of the application.	4.5	More Details
CVE-2022-36925	Zoom Rooms for macOS clients before version 5.11.4 contain an insecure key generation mechanism. The encryption key used for IPC between the Zoom Rooms daemon service and the Zoom Rooms client was generated using parameters that could be obtained by a local low-privileged application. That key can then be used to interact with the daemon service to execute privileged functions and cause a local denial of service.	4.4	More Details
CVE-2022-38482	A link-manipulation issue was discovered in Mega HOPEX 15.2.0.6110 before V5CP4.	4.3	More Details
CVE-2022-45164	An issue was discovered in Archibus Web Central 2022.03.01.107. A service exposed by the application allows a basic user to cancel (delete) a booking, created by someone else - even if this basic user is not a member of the booking	4.3	More Details
CVE-2022-45167	An issue was discovered in Archibus Web Central 2022.03.01.107. A service exposed by the application allows a basic user to access the profile information of all connected users.	4.3	More Details
CVE-2022-42435	IBM Business Automation Workflow 18.0.0, 18.0.1, 18.0.2, 19.0.1, 19.0.2, 19.0.3, 20.0.1, 20.0.2, 20.0.3, 21.0.1, 21.0.2, 21.0.3, and 22.0.1 is vulnerable to cross-site request forgery which could allow an attacker to execute malicious and unauthorized actions transmitted from a user that the website trusts. IBM X-Force ID: 238054.	4.3	More Details
CVE-2023-0141	Insufficient policy enforcement in CORS in Google Chrome prior to 109.0.5414.74 allowed a remote attacker to leak cross-origin data via a crafted HTML page. (Chromium security severity: Low)	4.3	More Details
CVE-2022-4103	The Royal Elementor Addons WordPress plugin before 1.3.56 does not have authorisation and CSRF checks when creating a template, and does not ensure that the post created is a template. This could allow any authenticated users, such as subscriber to create a post (as well as any post type) with an arbitrary title	4.3	More Details
CVE-2017-20162	A vulnerability, which was classified as problematic, has been found in vercel ms up to 1.x. This issue affects the function parse of the file index.js. The manipulation of the argument str leads to inefficient regular expression complexity. The attack may be initiated remotely. The exploit has been disclosed to the public and may be used. Upgrading to version 2.0.0 is able to address this issue. The patch is named caae2988ba2a37765d055c4eee63d383320ee662. It is recommended to upgrade the affected component. The associated identifier of this vulnerability is VDB-217451.	4.3	More Details

CVE Number	Description	Base Score	Reference
CVE-2022-1102	A vulnerability classified as problematic has been found in SourceCodester Royale Event Management System 1.0. Affected is an unknown function of the file /royal_event/companyprofile.php. The manipulation of the argument companyname/regno/companyaddress/companyemail leads to cross site scripting. It is possible to launch the attack remotely. VDB-195786 is the identifier assigned to this vulnerability.	4.3	More Details
CVE-2014-125066	A vulnerability was found in emmflo yuko-bot. It has been declared as problematic. This vulnerability affects unknown code. The manipulation of the argument title leads to denial of service. The attack can be initiated remotely. The name of the patch is e580584b877934a4298d4dd0c497c79e579380d0. It is recommended to apply a patch to fix this issue. The identifier of this vulnerability is VDB-217636.	4.3	More Details
CVE-2014-125069	A vulnerability was found in saxman maps-js-icoads. It has been classified as problematic. Affected is an unknown function. The manipulation leads to exposure of information through directory listing. It is possible to launch the attack remotely. The name of the patch is 34b8b0cce2807b119f4cffda2ac48fc8f427d69a. It is recommended to apply a patch to fix this issue. The identifier of this vulnerability is VDB-217644.	4.3	More Details
CVE-2022-4881	A vulnerability was found in CapsAdmin PAC3. It has been rated as problematic. Affected by this issue is some unknown functionality of the file lua/pac3/core/shared/http.lua. The manipulation of the argument url leads to cross site scripting. The attack may be launched remotely. The patch is identified as 8fc9e12dfa21d757be6eb4194c763e848b299ac0. It is recommended to apply a patch to fix this issue. VDB-217646 is the identifier assigned to this vulnerability.	4.3	More Details
CVE-2022-22337	IBM Sterling B2B Integrator Standard Edition 6.0.0.0 through 6.1.2.1 could disclose sensitive information to an authenticated user. IBM X-Force ID: 219507.	4.3	More Details
CVE-2020-36639	A vulnerability has been found in AlliedModders AMX Mod X on Windows and classified as critical. This vulnerability affects the function cmdVoteMap of the file plugins/adminvote.sma of the component Console Command Handler. The manipulation of the argument amx_votemap leads to path traversal. The patch is identified as a5f2b5539f6d61050b68df8b22ebb343a2862681. It is recommended to apply a patch to fix this issue. VDB-217354 is the identifier assigned to this vulnerability.	4.3	More Details
CVE-2022-3923	The ActiveCampaign for WooCommerce WordPress plugin before 1.9.8 does not have authorisation check when cleaning up its error logs via an AJAX action, which could allow any authenticated users, such as subscriber to call it and remove error logs.	4.3	More Details
CVE-2014-125054	A vulnerability classified as critical was found in koroket RedditOnRails. This vulnerability affects unknown code of the component Vote Handler. The manipulation leads to improper access controls. The attack can be initiated remotely. The patch is identified as 7f3c7407d95d532fcc342b00d68d0ea09ca71030. It is recommended to apply a patch to fix this issue. VDB-217594 is the identifier assigned to this vulnerability.	4.3	More Details
CVE-2022-4707	The Royal Elementor Addons plugin for WordPress is vulnerable to Cross-Site Request Forgery in versions up to, and including, 1.3.59. This is due to missing nonce validation in the 'wpr_create_mega_menu_template' AJAX function. This allows unauthenticated attackers to create Mega Menu templates, granted they can trick an administrator into performing an action, such as clicking a link.	4.3	More Details
CVE-2022-4711	The Royal Elementor Addons plugin for WordPress is vulnerable to insufficient access control in the 'wpr_save_mega_menu_settings' AJAX action in versions up to, and including, 1.3.59. This allows any authenticated user, including those with subscriber-level permissions, to enable and modify Mega Menu settings for any menu item.	4.3	More Details
CVE-2022-4701	The Royal Elementor Addons plugin for WordPress is vulnerable to insufficient access control in the 'wpr_activate_required_plugins' AJAX action in versions up to, and including, 1.3.59. This allows any authenticated user, including those with subscriber-level permissions, to activate the 'contact-form-7', 'media-library-assistant', or 'woocommerce' plugins if they are installed on the site.	4.3	More Details
CVE-2022-4703	The Royal Elementor Addons plugin for WordPress is vulnerable to insufficient access control in the 'wpr_reset_previous_import' AJAX action in versions up to, and including, 1.3.59. This allows any authenticated user, including those with subscriber-level permissions, to reset previously imported data.	4.3	More Details
CVE-2022-4426	The Mautic Integration for WooCommerce WordPress plugin before 1.0.3 does not have proper CSRF check when updating settings, and does not ensure that the options to be updated belong to the plugin, allowing attackers to make a logged in admin change arbitrary blog options via a CSRF attack.	4.3	More Details
CVE-2022-4705	The Royal Elementor Addons plugin for WordPress is vulnerable to insufficient access control in the 'wpr_final_settings_setup' AJAX action in versions up to, and including, 1.3.59. This allows any authenticated user, including those with subscriber-level permissions, to finalize activation of preset site configuration templates, which can be chosen and imported via a separate action documented in CVE-2022-4704.	4.3	More Details

CVE Number	Description	Base Score	Reference
CVE-2022-4709	The Royal Elementor Addons plugin for WordPress is vulnerable to insufficient access control in the 'wpr_import_library_template' AJAX action in versions up to, and including, 1.3.59. This allows any authenticated user, including those with subscriber-level permissions, to import and activate templates from the plugin's template library.	4.3	More Details
CVE-2022-4708	The Royal Elementor Addons plugin for WordPress is vulnerable to insufficient access control in the 'wpr_save_template_conditions' AJAX action in versions up to, and including, 1.3.59. This allows any authenticated user, including those with subscriber-level permissions, to modify the conditions under which templates are displayed.	4.3	More Details
CVE-2022-22470	IBM Security Verify Governance 10.0 stores user credentials in plain clear text which can be read by a local user. IBM X-Force ID: 225232.	4.1	More Details
CVE-2022-45126	Kernel subsystem within OpenHarmony-v3.1.4 and prior versions in kernel_liteos_a has a kernel stack overflow vulnerability when call SysClockGettime. 4 bytes padding data from kernel stack are copied to user space incorrectly and leaked.	4.0	More Details
CVE-2022-43662	Kernel subsystem within OpenHarmony-v3.1.4 and prior versions in kernel_liteos_a has a kernel stack overflow vulnerability when call SysTimerGettime. 4 bytes padding data from kernel stack are copied to user space incorrectly and leaked.	4.0	More Details
CVE-2022-4877	A vulnerability has been found in snoyberg keter up to 1.8.1 and classified as problematic. This vulnerability affects unknown code of the file Keter/Proxy.hs. The manipulation of the argument host leads to cross site scripting. The attack can be initiated remotely. Upgrading to version 1.8.2 is able to address this issue. The name of the patch is d41f3697926b231782a3ad8050f5af1ce5cc40b7. It is recommended to upgrade the affected component. The identifier of this vulnerability is VDB-217444.	3.5	More Details
CVE-2015-10013	A vulnerability was found in WebDevStudios taxonomy-switcher Plugin up to 1.0.3 on WordPress. It has been classified as problematic. Affected is the function taxonomy_switcher_init of the file taxonomy-switcher.php. The manipulation leads to cross site scripting. It is possible to launch the attack remotely. Upgrading to version 1.0.4 is able to address this issue. It is recommended to upgrade the affected component. VDB-217446 is the identifier assigned to this vulnerability.	3.5	More Details
CVE-2021-4305	A vulnerability was found in Woorank robots-txt-guard. It has been rated as problematic. Affected by this issue is the function makePathPattern of the file lib/patterns.js. The manipulation of the argument pattern leads to inefficient regular expression complexity. The exploit has been disclosed to the public and may be used. The name of the patch is c03827cd2f9933619c23894ce7c98401ea824020. It is recommended to apply a patch to fix this issue. The identifier of this vulnerability is VDB-217448.	3.5	More Details
CVE-2007-10001	A vulnerability classified as problematic has been found in web-cyradm. This affects an unknown part of the file search.php. The manipulation of the argument searchstring leads to sql injection. It is recommended to apply a patch to fix this issue. The identifier VDB-217449 was assigned to this vulnerability.	3.5	More Details
CVE-2022-46168	Discourse is an option source discussion platform. Prior to version 2.8.14 on the `stable` branch and version 2.9.0.beta15 on the `beta` and `tests-passed` branches, recipients of a group SMTP email could see the email addresses of all other users inside the group SMTP topic. Most of the time this is not an issue as they are likely already familiar with one another's email addresses. This issue is patched in versions 2.8.14 and 2.9.0.beta15. The fix is that someone sending emails out via group SMTP to non-staged users masks those emails with blind carbon copy (BCC). Staged users are ones that have likely only interacted with the group via email, and will likely include other people who were CC'd on the original email to the group. As a workaround, disable group SMTP for any groups that have it enabled.	3.5	More Details
CVE-2018-25065	A vulnerability was found in Wikimedia mediawiki-extensions-I18nTags and classified as problematic. This issue affects some unknown processing of the file I18nTags_body.php of the component Unlike Parser. The manipulation leads to cross site scripting. The attack may be initiated remotely. The identifier of the patch is b4bc3cbbb099eab50cf2b544cf577116f1867b94. It is recommended to apply a patch to fix this issue. The identifier VDB-217445 was assigned to this vulnerability.	3.5	More Details
CVE-2014-125039	A vulnerability, which was classified as problematic, has been found in kkokko NeoXplora. Affected by this issue is some unknown functionality of the component Trainer Handler. The manipulation leads to cross site scripting. The attack may be launched remotely. The name of the patch is dce1aecd6ee050a29f953ffd8f02f21c7c13f1e6. It is recommended to apply a patch to fix this issue. The identifier of this vulnerability is VDB-217352.	3.5	More Details
CVE-2022-4869	A vulnerability was found in Evolution Events Artaxerxes. It has been declared as problematic. This vulnerability affects unknown code of the file arta/common/middleware.py of the component POST Parameter Handler. The manipulation of the argument password leads to information disclosure. The attack can be initiated remotely. The patch is identified as 022111407d34815c16c6eada2de69ca34084dc0d. It is recommended to apply a patch to fix this issue. VDB-217438 is the identifier assigned to this vulnerability.	3.5	More Details

CVE Number	Description	Base Score	Reference
CVE-2018-25064	A vulnerability was found in OSM Lab show-me-the-way. It has been rated as problematic. This issue affects some unknown processing of the file js/site.js. The manipulation leads to cross site scripting. The attack may be initiated remotely. The patch is named 4bed3b34dcc01fe6661f39c0e5d2285b340f7cac. It is recommended to apply a patch to fix this issue. The associated identifier of this vulnerability is VDB-217439.	3.5	More Details
CVE-2016-15010	** UNSUPPORTED WHEN ASSIGNED ** A vulnerability classified as problematic was found in University of Cambridge django-ucamlookup up to 1.9.1. Affected by this vulnerability is an unknown functionality of the component Lookup Handler. The manipulation leads to cross site scripting. The attack can be launched remotely. Upgrading to version 1.9.2 is able to address this issue. The identifier of the patch is 5e25e4765637ea4b9e0bf5fcd5e9a922abee7eb3. It is recommended to upgrade the affected component. The identifier VDB-217441 was assigned to this vulnerability. NOTE: This vulnerability only affects products that are no longer supported by the maintainer.	3.5	More Details
CVE-2016-15009	A vulnerability classified as problematic has been found in OpenACS bug-tracker. Affected is an unknown function of the file lib/nav-bar.adp of the component Search. The manipulation leads to cross-site request forgery. It is possible to launch the attack remotely. The name of the patch is aee43e5714cd8b697355ec3bf83eefee176d3fc3. It is recommended to apply a patch to fix this issue. The identifier of this vulnerability is VDB-217440.	3.5	More Details
CVE-2015-10019	A vulnerability, which was classified as problematic, has been found in foxoverflow MySimplifiedSQL. This issue affects some unknown processing of the file MySimplifiedSQL_Examples.php. The manipulation of the argument FirstName/LastName leads to cross site scripting. The attack may be initiated remotely. The patch is named 3b7481c72786f88041b7c2d83bb4f219f77f1293. It is recommended to apply a patch to fix this issue. The associated identifier of this vulnerability is VDB-217595.	3.5	More Details
CVE-2019-25095	A vulnerability, which was classified as problematic, was found in kakwa LdapCherry up to 0.x. Affected is an unknown function of the component URL Handler. The manipulation leads to cross site scripting. It is possible to launch the attack remotely. Upgrading to version 1.0.0 is able to address this issue. The patch is identified as 6f98076281e9452fdb1adcd1bcbb70a6f968ade9. It is recommended to upgrade the affected component. VDB-217434 is the identifier assigned to this vulnerability.	3.5	More Details
CVE-2022-4876	A vulnerability was found in Kaltura mwEmbed up to 2.96.rc1 and classified as problematic. This issue affects some unknown processing of the file includes/DefaultSettings.php. The manipulation of the argument HTTP_X_FORWARDED_HOST leads to cross site scripting. The attack may be initiated remotely. Upgrading to version 2.96.rc2 is able to address this issue. The patch is named 13b8812ebc8c9fa034eed91ab35ba8423a528c0b. It is recommended to upgrade the affected component. The associated identifier of this vulnerability is VDB-217427.	3.5	More Details
CVE-2021-4302	A vulnerability was found in slackero phpwcms up to 1.9.26. It has been classified as problematic. This affects an unknown part of the component SVG File Handler. The manipulation leads to cross site scripting. It is possible to initiate the attack remotely. Upgrading to version 1.9.27 is able to address this issue. The patch is named b39db9c7ad3800f319195ff0e26a0981395b1c54. It is recommended to upgrade the affected component. The associated identifier of this vulnerability is VDB-217419.	3.5	More Details
CVE-2019-25094	A vulnerability, which was classified as problematic, was found in innologi appointments Extension up to 2.0.5 on TYPO3. This affects an unknown part of the component Appointment Handler. The manipulation of the argument formfield leads to cross site scripting. It is possible to initiate the attack remotely. Upgrading to version 2.0.6 is able to address this issue. The identifier of the patch is 986d3cb34e5e086c6f04e061f600ffc5837abe7f. It is recommended to upgrade the affected component. The identifier VDB-217353 was assigned to this vulnerability.	3.5	More Details
CVE-2016-15008	A vulnerability was found in oxguy3 coebot-www and classified as problematic. This issue affects the function displayChannelCommands/displayChannelQuotes/displayChannelAutoreplies/showChannelHighlights/showChannelBoir of the file js/channel.js. The manipulation leads to cross site scripting. The attack may be initiated remotely. The patch is named c1a6c44092585da4236237e0e7da94ee2996a0ca. It is recommended to apply a patch to fix this issue. The associated identifier of this vulnerability is VDB-217355.	3.5	More Details
CVE-2019-25096	A vulnerability has been found in soerennb eXtplorer up to 2.1.12 and classified as problematic. Affected by this vulnerability is an unknown functionality. The manipulation leads to cross site scripting. The attack can be launched remotely. Upgrading to version 2.1.13 is able to address this issue. The patch is named b8fcb888f4ff5e171c16797a4b075c6c6f50bf46. It is recommended to upgrade the affected component. The associated identifier of this vulnerability is VDB-217435.	3.5	More Details
CVE-2015-10028	A vulnerability has been found in ss15-this-is-sparta and classified as problematic. This vulnerability affects unknown code of the file js/roomElement.js of the component Main Page. The manipulation leads to cross site scripting. The attack can be initiated remotely. The name of the patch is ba2f71ad3a46e5949ee0c510b544fa4ea973baaa. It is recommended to apply a patch to fix this issue. The identifier of this vulnerability is VDB-217624.	3.5	More Details

CVE Number	Description	Base Score	Reference
CVE-2021-4309	A vulnerability, which was classified as problematic, has been found in 01-Scripts 01ACP. This issue affects some unknown processing. The manipulation of the argument $_SERVER['SCRIPT_NAME'] leads to cross site scripting. The attack may be initiated remotely. The identifier of the patch is a16eb7da46ed22bc61067c212635394f2571d3c4. It is recommended to apply a patch to fix this issue. The identifier VDB-217649 was assigned to this vulnerability.	3.5	More Details
CVE-2015-10025	A vulnerability has been found in luelista miniConf up to 1.7.6 and classified as problematic. Affected by this vulnerability is an unknown functionality of the file miniConf/MessageView.cs of the component URL Scanning. The manipulation leads to denial of service. Upgrading to version 1.7.7 and 1.8.0 is able to address this issue. The patch is named c06c2e5116c306e4e1bc79779f0eda2d1182f655. It is recommended to upgrade the affected component. The associated identifier of this vulnerability is VDB-217615.	3.5	More Details
CVE-2021-4306	A vulnerability classified as problematic has been found in cronvel terminal-kit up to 2.1.7. Affected is an unknown function. The manipulation leads to inefficient regular expression complexity. Upgrading to version 2.1.8 is able to address this issue. The name of the patch is a2e446cc3927b559d0281683feb9b821e83b758c. It is recommended to upgrade the affected component. The identifier of this vulnerability is VDB-217620.	3.5	More Details
CVE-2020-36646	A vulnerability classified as problematic has been found in MediaArea ZenLib up to 0.4.38. This affects the function Ztring::Date_From_Seconds_1970_Local of the file Source/ZenLib/Ztring.cpp. The manipulation of the argument Value leads to unchecked return value to null pointer dereference. Upgrading to version 0.4.39 is able to address this issue. The identifier of the patch is 6475fcccd37c9cf17e0cfe263b5fe0e2e47a8408. It is recommended to upgrade the affected component. The identifier VDB-217629 was assigned to this vulnerability.	3.5	More Details
CVE-2014-125070	A vulnerability has been found in yanheven console and classified as problematic. Affected by this vulnerability is the function get_zone_hosts/AvailabilityZonesTable of the file openstack_dashboard/dashboards/admin/aggregates/tables.py. The manipulation leads to cross site scripting. The attack can be launched remotely. The patch is named ba908ae88d5925f4f6783eb234cc4ea95017472b. It is recommended to apply a patch to fix this issue. The associated identifier of this vulnerability is VDB-217651.	3.5	More Details
CVE-2010-10004	A vulnerability was found in Information Cards Module on simpleSAMLphp and classified as problematic. This issue affects some unknown processing. The manipulation leads to cross site scripting. The attack may be initiated remotely. Upgrading to version 1.0 is able to address this issue. The identifier of the patch is f6bfea49ae16dc6e179df8306d39c3694f1ef186. It is recommended to upgrade the affected component. The identifier VDB-217661 was assigned to this vulnerability.	3.5	More Details
CVE-2015-10032	A vulnerability was found in HealthMateWeb. It has been declared as problematic. Affected by this vulnerability is an unknown functionality of the file createaccount.php. The manipulation of the argument username/password/first_name/last_name/company/phone leads to cross site scripting. The attack can be launched remotely. The patch is named 472776c25b1046ecaf962c46fed7c713c72c28e3. It is recommended to apply a patch to fix this issue. The associated identifier of this vulnerability is VDB-217663.	3.5	More Details
CVE-2021-4310	A vulnerability was found in 01-Scripts 01-Artikelsystem. It has been classified as problematic. Affected is an unknown function of the file 01article.php. The manipulation of the argument $_SERVER['PHP_SELF'] leads to cross site scripting. It is possible to launch the attack remotely. The patch is identified as ae849b347a58c2cb1be38d04bbe56fc883d5d84a. It is recommended to apply a patch to fix this issue. VDB-217662 is the identifier assigned to this vulnerability.	3.5	More Details
CVE-2017-20165	A vulnerability classified as problematic has been found in debug-js debug up to 3.0.x. This affects the function useColors of the file src/node.js. The manipulation of the argument str leads to inefficient regular expression complexity. Upgrading to version 3.1.0 is able to address this issue. The identifier of the patch is c38a0166c266a679c8de012d4eaccec3f944e685. It is recommended to upgrade the affected component. The identifier VDB-217665 was assigned to this vulnerability.	3.5	More Details
CVE-2022-4884	Path-Traversal in MKP storing in Tribe29 Checkmk <=2.0.0p32 and <= 2.1.0p18 allows an administrator to write mkp files to arbitrary locations via a malicious mkp file.	3.5	More Details
CVE-2015-10033	A vulnerability, which was classified as problematic, was found in jvvlee MerlinsBoard. This affects an unknown part of the component Grade Handler. The manipulation leads to improper authorization. The identifier of the patch is 134f5481e2914b7f096cd92a22b1e6bcb8e6dfe5. It is recommended to apply a patch to fix this issue. The identifier VDB-217713 was assigned to this vulnerability.	3.5	More Details
CVE-2022-3343	The WPQA Builder WordPress plugin before 5.9.3 (which is a companion plugin used with Discy and Himer Discy WordPress themes) incorrectly tries to validate that a user already follows another in the wpqa_following_you_ajax action, allowing a user to inflate their score on the site by having another user send repeated follow actions to them.	3.5	More Details

CVE Number	Description	Base Score	Reference
CVE-2015-10021	A vulnerability was found in ritterim definely. It has been classified as problematic. Affected is an unknown function of the file src/database.js. The manipulation leads to cross site scripting. It is possible to launch the attack remotely. The name of the patch is b31a022ba4d8d17148445a13ebb5a42ad593dbaa. It is recommended to apply a patch to fix this issue. The identifier of this vulnerability is VDB-217608.	3.5	More Details
CVE-2020-36644	A vulnerability has been found in jamesmartin Inline SVG up to 1.7.1 and classified as problematic. Affected by this vulnerability is an unknown functionality of the file lib/inline_svg/action_view/helpers.rb of the component URL Parameter Handler. The manipulation of the argument filename leads to cross site scripting. The attack can be launched remotely. Upgrading to version 1.7.2 is able to address this issue. The identifier of the patch is f5363b351508486021f99e083c92068cf2943621. It is recommended to upgrade the affected component. The identifier VDB-217597 was assigned to this vulnerability.	3.5	More Details
CVE-2023-21759	Windows Smart Card Resource Management Server Security Feature Bypass Vulnerability	3.3	More Details
CVE-2016-15014	A vulnerability has been found in CESNET theme-cesnet up to 1.x on ownCloud and classified as problematic. Affected by this vulnerability is an unknown functionality of the file cesnet/core/lostpassword/templates/resetpassword.php. The manipulation leads to insufficiently protected credentials. Attacking locally is a requirement. Upgrading to version 2.0.0 is able to address this issue. The identifier of the patch is 2b857f2233ce5083b4d5bc9bfc4152f933c3e4a6. It is recommended to upgrade the affected component. The identifier VDB-217633 was assigned to this vulnerability.	3.3	More Details
CVE-2023-0114	A vulnerability was found in Netis Netcore Router. It has been rated as problematic. Affected by this issue is some unknown functionality of the file param.file.tgz of the component Backup Handler. The manipulation leads to cleartext storage in a file or on disk. Local access is required to approach this attack. The identifier of this vulnerability is VDB-217592.	3.3	More Details
CVE-2022-4102	The Royal Elementor Addons WordPress plugin before 1.3.56 does not have authorization and CSRF checks when deleting a template and does not ensure that the post to be deleted is a template. This could allow any authenticated users, such as subscribers, to delete arbitrary posts assuming they know the related slug.	3.1	More Details
CVE-2022-43573	IBM Robotic Process Automation 20.12 through 21.0.6 is vulnerable to exposure of the name and email for the creator/modifier of platform level objects. IBM X-Force ID: 238678.	3.1	More Details
CVE-2014-125057	A vulnerability was found in mrobit robitailletheknot. It has been classified as problematic. This affects an unknown part of the file app/filters.php of the component CSRF Token Handler. The manipulation of the argument _token leads to incorrect comparison. It is possible to initiate the attack remotely. The complexity of an attack is rather high. The exploitability is told to be difficult. The patch is named 6b2813696ccb88d0576dfb305122ee880eb36197. It is recommended to apply a patch to fix this issue. The associated identifier of this vulnerability is VDB-217599.	3.1	More Details
CVE-2014-125056	A vulnerability was found in Pylons horus and classified as problematic. Affected by this issue is some unknown functionality of the file horus/flows/local/services.py. The manipulation leads to observable timing discrepancy. The complexity of an attack is rather high. The exploitation is known to be difficult. The patch is identified as fd56ccb62ce3cbdab0484fe4f9c25c4eda6c57ec. It is recommended to apply a patch to fix this issue. VDB-217598 is the identifier assigned to this vulnerability.	2.6	More Details
CVE-2014-125055	A vulnerability, which was classified as problematic, was found in agnivade easy-scrypt. Affected is the function VerifyPassphrase of the file scrypt.go. The manipulation leads to observable timing discrepancy. The complexity of an attack is rather high. The exploitability is told to be difficult. Upgrading to version 1.0.0 is able to address this issue. The name of the patch is 477c10cf3b144ddf96526aa09f5fdea613f21812. It is recommended to upgrade the affected component. The identifier of this vulnerability is VDB-217596.	2.6	More Details
CVE-2022-4882	A vulnerability was found in kaltura mwEmbed up to 2.91. It has been rated as problematic. Affected by this issue is some unknown functionality of the file modules/KalturaSupport/components/share/share.js of the component Share Plugin. The manipulation of the argument res leads to cross site scripting. The attack may be launched remotely. The complexity of an attack is rather high. The exploitation is known to be difficult. The exploit has been disclosed to the public and may be used. Upgrading to version 2.92.rc1 is able to address this issue. The name of the patch is 4f11b6f6610acd6d89de5f8be47cf7c610643845. It is recommended to upgrade the affected component. The identifier of this vulnerability is VDB-217664.	2.6	More Details
CVE-2016-15015	A vulnerability, which was classified as problematic, was found in viafintech Barzahlen Payment Module PHP SDK up to 2.0.0. Affected is the function verify of the file src/Webhook.php. The manipulation leads to observable timing discrepancy. The complexity of an attack is rather high. The exploitability is told to be difficult. Upgrading to version 2.0.1 is able to address this issue. The patch is identified as 3e7d29dc0ca6c054a6d6e211f32dae89078594c1. It is recommended to upgrade the affected component. VDB-217650 is the identifier assigned to this vulnerability.	2.6	More Details

CVE Number	Description	Base Score	Reference
CVE-2023-0125	A vulnerability was found in Control iD Gerencia Web 1.30. It has been declared as problematic. Affected by this vulnerability is an unknown functionality of the component Web Interface. The manipulation of the argument Nome leads to cross site scripting. The attack can be launched remotely. The exploit has been disclosed to the public and may be used. The identifier VDB-217717 was assigned to this vulnerability.	2.4	More Details
CVE-2022-4875	A vulnerability has been found in fossology and classified as problematic. This vulnerability affects unknown code. The manipulation of the argument sql/VarValue leads to cross site scripting. The attack can be initiated remotely. The patch is identified as 8e0eba001662c7eb35f045b70dd458a4643b4553. It is recommended to apply a patch to fix this issue. VDB-217426 is the identifier assigned to this vulnerability.	2.4	More Details
CVE-2023-22473	Talk-Android enables users to have video & audio calls through Nextcloud on Android. Due to passcode bypass, an attacker is able to access the user's Nextcloud files and view conversations. To exploit this the attacker needs to have physical access to the target's device. There are currently no known workarounds available. It is recommended that the Nextcloud Talk Android app is upgraded to 15.0.2.	2.1	More Details
CVE-2021-4303	A vulnerability, which was classified as problematic, has been found in shannah Xataface up to 2.x. Affected by this issue is the function testftp of the file install/install_form.js.php of the component Installer. The manipulation leads to cross site scripting. The attack may be launched remotely. The complexity of an attack is rather high. The exploitation is known to be difficult. Upgrading to version 3.0.0 is able to address this issue. The patch is identified as 94143a4299e386f33bf582139cd4702571d93bde. It is recommended to upgrade the affected component. VDB-217442 is the identifier assigned to this vulnerability. NOTE: Installer is disabled by default.	2.0	More Details
CVE-2022-44537	Rejected reason: CVE was unused by HPE.	N/A	More Details
CVE-2020-24645	Rejected reason: CVE was unused by HPE.	N/A	More Details
CVE-2020-7112	Rejected reason: CVE was unused by HPE.	N/A	More Details
CVE-2022-29899	Rejected reason: DO NOT USE THIS CANDIDATE NUMBER. ConsultIDs: none. Reason: This candidate was in a CNA pool that was not assigned to any issues during 2022. Notes: none.	N/A	More Details
CVE-2022-0259	Rejected reason: DO NOT USE THIS CANDIDATE NUMBER. ConsultIDs: none. Reason: This candidate was in a CNA pool that was not assigned to any issues during 2022. Notes: none.	N/A	More Details
CVE-2021-41986	Rejected reason: DO NOT USE THIS CANDIDATE NUMBER. ConsultIDs: none. Reason: This candidate was in a CNA pool that was not assigned to any issues during 2021. Notes: none.	N/A	More Details
CVE-2021-41984	Rejected reason: DO NOT USE THIS CANDIDATE NUMBER. ConsultIDs: none. Reason: This candidate was in a CNA pool that was not assigned to any issues during 2021. Notes: none.	N/A	More Details
CVE-2021-41985	Rejected reason: DO NOT USE THIS CANDIDATE NUMBER. ConsultIDs: none. Reason: This candidate was in a CNA pool that was not assigned to any issues during 2021. Notes: none.	N/A	More Details
CVE-2021-25222	Rejected reason: DO NOT USE THIS CANDIDATE NUMBER. ConsultIDs: none. Reason: This candidate is unused by its CNA. Notes: none.	N/A	More Details
CVE-2021-41983	Rejected reason: DO NOT USE THIS CANDIDATE NUMBER. ConsultIDs: none. Reason: This candidate was in a CNA pool that was not assigned to any issues during 2021. Notes: none.	N/A	More Details
CVE-2021-41982	Rejected reason: DO NOT USE THIS CANDIDATE NUMBER. ConsultIDs: none. Reason: This candidate was in a CNA pool that was not assigned to any issues during 2021. Notes: none.	N/A	More Details

CVE Number	Description	Base Score	Reference
CVE-2021-41981	Rejected reason: DO NOT USE THIS CANDIDATE NUMBER. ConsultIDs: none. Reason: This candidate was in a CNA pool that was not assigned to any issues during 2021. Notes: none.	N/A	More Details
CVE-2021-41980	Rejected reason: DO NOT USE THIS CANDIDATE NUMBER. ConsultIDs: none. Reason: This candidate was in a CNA pool that was not assigned to any issues during 2021. Notes: none.	N/A	More Details
CVE-2021-41979	Rejected reason: DO NOT USE THIS CANDIDATE NUMBER. ConsultIDs: none. Reason: This candidate was in a CNA pool that was not assigned to any issues during 2021. Notes: none.	N/A	More Details
CVE-2021-41978	Rejected reason: DO NOT USE THIS CANDIDATE NUMBER. ConsultIDs: none. Reason: This candidate was in a CNA pool that was not assigned to any issues during 2021. Notes: none.	N/A	More Details
CVE-2021-41977	Rejected reason: DO NOT USE THIS CANDIDATE NUMBER. ConsultIDs: none. Reason: This candidate was in a CNA pool that was not assigned to any issues during 2021. Notes: none.	N/A	More Details
CVE-2020-7118	Rejected reason: CVE was unused by HPE.	N/A	More Details
CVE-2020-36643	Rejected reason: DO NOT USE THIS CANDIDATE NUMBER. ConsultIDs: none. Reason: This candidate was withdrawn by its CNA. Further investigation showed that it was not a security issue. Notes: none.	N/A	More Details
CVE-2021-25221	Rejected reason: DO NOT USE THIS CANDIDATE NUMBER. ConsultIDs: none. Reason: This candidate is unused by its CNA. Notes: none.	N/A	More Details
CVE-2022-46336	Rejected reason: DO NOT USE THIS CANDIDATE NUMBER. ConsultIDs: none. Reason: This candidate is unused by its CNA. Notes: none.	N/A	More Details
CVE-2021-25223	Rejected reason: DO NOT USE THIS CANDIDATE NUMBER. ConsultIDs: none. Reason: This candidate is unused by its CNA. Notes: none.	N/A	More Details
CVE-2022-44540	Rejected reason: CVE was unused by HPE.	N/A	More Details
CVE-2021-41010	Rejected reason: CVE was unused by HPE.	N/A	More Details
CVE-2021-41009	Rejected reason: CVE was unused by HPE.	N/A	More Details
CVE-2021-41008	Rejected reason: CVE was unused by HPE.	N/A	More Details
CVE-2021-41007	Rejected reason: CVE was unused by HPE.	N/A	More Details
CVE-2021-41006	Rejected reason: CVE was unused by HPE.	N/A	More Details
CVE-2014-125043	Rejected reason: DO NOT USE THIS CANDIDATE NUMBER. ConsultIDs: none. Reason: This candidate was withdrawn by its CNA. Further investigation showed that it was not a security issue. Notes: none.	N/A	More Details

CVE Number	Description	Base Score	Reference
CVE-2014-125042	Rejected reason: DO NOT USE THIS CANDIDATE NUMBER. ConsultIDs: none. Reason: This candidate was withdrawn by its CNA. Further investigation showed that it was not a security issue. Notes: none.	N/A	More Details
CVE-2022-44538	Rejected reason: CVE was unused by HPE.	N/A	More Details
CVE-2022-44539	Rejected reason: CVE was unused by HPE.	N/A	More Details
CVE-2014-125064	Rejected reason: DO NOT USE THIS CANDIDATE NUMBER. ConsultIDs: none. Reason: This candidate was withdrawn by its CNA. Further investigation showed that it was not a security issue. Notes: none.	N/A	More Details
CVE-2022-46335	Rejected reason: DO NOT USE THIS CANDIDATE NUMBER. ConsultIDs: none. Reason: This candidate is unused by its CNA. Notes: none.	N/A	More Details
CVE-2022-44541	Rejected reason: CVE was unused by HPE.	N/A	More Details
CVE-2022-45614	Rejected reason: DO NOT USE THIS CANDIDATE NUMBER. ConsultIDs: CVE-2022-4228. Reason: This candidate is a reservation duplicate of CVE-2022-4228. Notes: All CVE users should reference CVE-2022-4228 instead of this candidate. All references and descriptions in this candidate have been removed to prevent accidental usage.	N/A	More Details
CVE-2019-5316	Rejected reason: CVE was unused by HPE.	N/A	More Details
CVE-2019-5325	Rejected reason: CVE was unused by HPE.	N/A	More Details
CVE-2022-45883	Rejected reason: DO NOT USE THIS CANDIDATE NUMBER. ConsultIDs: none. Reason: This candidate is unused by its CNA. Notes: none.	N/A	More Details
CVE-2020-24642	Rejected reason: CVE was unused by HPE.	N/A	More Details
CVE-2020-24643	Rejected reason: CVE was unused by HPE.	N/A	More Details
CVE-2020-24644	Rejected reason: CVE was unused by HPE.	N/A	More Details
CVE-2022-44536	Rejected reason: CVE was unused by HPE.	N/A	More Details
CVE-2019-5313	Rejected reason: CVE was unused by HPE.	N/A	More Details