SingCERT
Singapore Cyber Emergency Response Team

Security Bulletin 12 July 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-2022-4361	Keycloak, an open-source identity and access management solution, has a cross-site scripting (XSS) vulnerability in the SAML or OIDC providers. The vulnerability can allow an attacker to execute malicious scripts by setting the AssertionConsumerServiceURL value or the redirect_uri.	10.0	More Details
CVE-2021-32494	Radare2 has a division by zero vulnerability in Mach-O parser's rebase_buffer function. This allow attackers to create malicious inputs that can cause denial of service.	10.0	More Details
CVE-2021-33796	In MuJS before version 1.1.2, a use-after-free flaw in the regexp source property access may cause denial of service.	10.0	More Details
CVE-2021-32495	Radare2 has a use-after-free vulnerability in pyc parser's get_none_object function. Attacker can read freed memory afterwards. This will allow attackers to cause denial of service.	10.0	More Details

CVE Number	Description	Base Score	Reference
CVE-2023-36460	Mastodon is a free, open-source social network server based on ActivityPub. Starting in version 3.5.0 and prior to versions 3.5.9, 4.0.5, and 4.1.3, attackers using carefully crafted media files can cause Mastodon's media processing code to create arbitrary files at any location. This allows attackers to create and overwrite any file Mastodon has access to, allowing Denial of Service and arbitrary Remote Code Execution. Versions 3.5.9, 4.0.5, and 4.1.3 contain a patch for this issue.	9.9	More Details
CVE-2023-29130	A vulnerability has been identified in SIMATIC CN 4100 (All versions < V2.5). Affected device consists of improper access controls in the configuration files that leads to privilege escalation. An attacker could gain admin access with this vulnerability leading to complete device control.	9.9	More Details
CVE-2023-37172	TOTOLINK A3300R V17.0.0cu.557_B20221024 was discovered to contain a command injection vulnerability via the ip parameter in the setDiagnosisCfg function.	9.8	More Details
CVE-2023-37173	TOTOLINK A3300R V17.0.0cu.557_B20221024 was discovered to contain a command injection vulnerability via the command parameter in the setTracerouteCfg function.	9.8	More Details
CVE-2021-46891	Vulnerability of incomplete read and write permission verification in the GPU module. Successful exploitation of this vulnerability may affect service confidentiality, integrity, and availability.	9.8	More Details
CVE-2023-2046	Improper Neutralization of Special Elements used in an SQL Command ('SQL Injection') vulnerability in Yontem Informatics Vehicle Tracking System allows SQL Injection.This issue affects Vehicle Tracking System: before 8.	9.8	More Details
CVE-2023-37702	Tenda FH1203 V2.0.1.6 was discovered to contain a stack overflow via the deviceId parameter in the formSetDeviceName function.	9.8	More Details
CVE-2023-2852	Improper Neutralization of Special Elements used in an SQL Command ('SQL Injection') vulnerability in Softmed SelfPatron allows SQL Injection.This issue affects SelfPatron : before 2.0.	9.8	More Details
CVE-2023-32254	A flaw was found in the Linux kernel's ksmbd, a high-performance in-kernel SMB server. The specific flaw exists within the processing of SMB2_TREE_DISCONNECT commands. The issue results from the lack of proper locking when performing operations on an object. An attacker can leverage this vulnerability to execute code in the context of the kernel.	9.8	More Details

CVE Number	Description	Base Score	Reference
CVE-2023-37152	Projectworlds Online Art Gallery Project 1.0 allows unauthenticated users to perform arbitrary file uploads via the adminHome.php page. Note: This has been disputed as not a valid vulnerability.	9.8	More Details
CVE-2023-3045	Improper Neutralization of Special Elements used in an SQL Command ('SQL Injection') vulnerability in Tise Technology Parking Web Report allows SQL Injection.This issue affects Parking Web Report: before 2.1.	9.8	More Details
CVE-2023-3076	The MStore API WordPress plugin before 3.9.9 does not prevent visitors from creating user accounts with the role of their choice via their wholesale REST API endpoint. This is only exploitable if the site owner paid to access the plugin's pro features.	9.8	More Details
CVE-2023-37171	TOTOLINK A3300R V17.0.0cu.557_B20221024 was discovered to contain a command injection vulnerability via the admuser parameter in the setPasswordCfg function.	9.8	More Details
CVE-2023-3077	The MStore API WordPress plugin before 3.9.8 does not sanitise and escape a parameter before using it in a SQL statement, leading to a Blind SQL injection exploitable by unauthenticated users. This is only exploitable if the site owner elected to pay to get access to the plugins' pro features, and uses the woocommerce-appointments plugin.	9.8	More Details
CVE-2023-37700	Tenda FH1203 V2.0.1.6 was discovered to contain a stack overflow via the ssid parameter in the form_fast_setting_wifi_set function.	9.8	More Details
CVE-2023-37701	Tenda FH1203 V2.0.1.6 was discovered to contain a stack overflow via the deviceId parameter in the addWifiMacFilter function.	9.8	More Details
CVE-2021-46890	Vulnerability of incomplete read and write permission verification in the GPU module. Successful exploitation of this vulnerability may affect service confidentiality, integrity, and availability.	9.8	More Details
CVE-2023-37170	TOTOLINK A3300R V17.0.0cu.557_B20221024 was discovered to contain an unauthenticated remote code execution (RCE) vulnerability via the lang parameter in the setLanguageCfg function.	9.8	More Details
CVE-2023-34561	A buffer overflow in the level parsing code of RobTop Games AB Geometry Dash v2.113 allows attackers to execute arbitrary code via entering a Geometry Dash level.	9.8	More Details
CVE-2023-35367	Windows Routing and Remote Access Service (RRAS) Remote Code Execution Vulnerability	9.8	More Details

CVE Number	Description	Base Score	Reference
CVE-2023-35366	Windows Routing and Remote Access Service (RRAS) Remote Code Execution Vulnerability	9.8	More Details
CVE-2023-35365	Windows Routing and Remote Access Service (RRAS) Remote Code Execution Vulnerability	9.8	More Details
CVE-2023-32057	Microsoft Message Queuing (MSMQ) Remote Code Execution Vulnerability	9.8	More Details
CVE-2023-26861	SQL injection vulnerability found in PrestaShop vivawallet v.1.7.10 and before allows a remote attacker to gain privileges via the vivawallet() module.	9.8	More Details
CVE-2023-37659	xalpha v0.11.4 is vulnerable to Remote Command Execution (RCE).	9.8	More Details
CVE-2023-37656	WebsiteGuide v0.2 is vulnerable to Remote Command Execution (RCE) via image upload.	9.8	More Details
CVE-2023-24489	A vulnerability has been discovered in the customer-managed ShareFile storage zones controller which, if exploited, could allow an unauthenticated attacker to remotely compromise the customer-managed ShareFile storage zones controller.	9.8	More Details
CVE-2023-37704	Tenda FH1203 V2.0.1.6 was discovered to contain a stack overflow via the deviceId parameter in the formSetClientState function.	9.8	More Details
CVE-2023-34347	Delta Electronics InfraSuite Device Master versions prior to 1.0.7 contains classes that cannot be deserialized, which could allow an attack to remotely execute arbitrary code.	9.8	More Details
CVE-2023-37712	Tenda AC1206 V15.03.06.23, F1202 V1.2.0.20(408), and FH1202 V1.2.0.20(408) were discovered to contain a stack overflow in the page parameter in the fromSetIpBind function.	9.8	More Details
CVE-2023-37711	Tenda AC1206 V15.03.06.23 and AC10 V15.03.06.47 were discovered to contain a stack overflow in the deviceId parameter in the saveParentControlInfo function.	9.8	More Details

CVE Number	Description	Base Score	Reference
CVE-2023-37710	Tenda AC1206 V15.03.06.23 and AC10 V15.03.06.47 were discovered to contain a stack overflow in the wpapsk_crypto parameter in the fromSetWirelessRepeat function.	9.8	More Details
CVE-2023-37707	Tenda FH1203 V2.0.1.6 was discovered to contain a stack overflow via the page parameter in the fromVirtualSer function.	9.8	More Details
CVE-2023-37706	Tenda FH1203 V2.0.1.6 was discovered to contain a stack overflow via the entrys parameter in the fromAddressNat function.	9.8	More Details
CVE-2023-37705	Tenda FH1203 V2.0.1.6 was discovered to contain a stack overflow via the page parameter in the fromAddressNat function.	9.8	More Details
CVE-2023-37703	Tenda FH1203 V2.0.1.6 was discovered to contain a stack overflow via the speed_dir parameter in the formSetSpeedWan function.	9.8	More Details
CVE-2023-37286	SmartSoft SmartBPM.NET has a vulnerability of using hard-coded machine key. An unauthenticated remote attacker can use the machine key to send serialized payload to the server to execute arbitrary code and disrupt service.	9.8	More Details
CVE-2023-36994	In TravianZ 8.3.4 and 8.3.3, Incorrect Access Control in the installation script allows an attacker to overwrite the server configuration and inject PHP code.	9.8	More Details
CVE-2023-29382	An issue in Zimbra Collaboration ZCS v.8.8.15 and v.9.0 allows an attacker to execute arbitrary code via the sfdc_preauth.jsp component.	9.8	More Details
CVE-2023-36665	"protobuf.js (aka protobufjs) 6.10.0 through 7.x before 7.2.5 allows Prototype Pollution, a different vulnerability than CVE-2022-25878. A user-controlled protobuf message can be used by an attacker to pollute the prototype of Object.prototype by adding and overwriting its data and functions. Exploitation can involve: (1) using the function parse to parse protobuf messages on the fly, (2) loading .proto files by using load/loadSync functions, or (3) providing untrusted input to the functions ReflectionObject.setParsedOption and util.setProperty.	9.8	More Details
CVE-2020-25969	gnuplot v5.5 was discovered to contain a buffer overflow via the function plotrequest().	9.8	More Details

CVE Number	Description	Base Score	Reference
CVE-2022-46080	Nexxt Nebula 1200-AC 15.03.06.60 allows authentication bypass and command execution by using the HTTPD service to enable TELNET.	9.8	More Details
CVE-2021-46894	Use After Free (UAF) vulnerability in the uinput module.Successful exploitation of this vulnerability may lead to kernel privilege escalation.	9.8	More Details
CVE-2022-48510	Input verification vulnerability in the AMS module. Successful exploitation of this vulnerability will cause unauthorized operations.	9.8	More Details
CVE-2022-48511	Use After Free (UAF) vulnerability in the audio PCM driver module under special conditions. Successful exploitation of this vulnerability may cause audio features to perform abnormally.	9.8	More Details
CVE-2022-48512	Use After Free (UAF) vulnerability in the Vdecoderservice service. Successful exploitation of this vulnerability may cause the image decoding feature to perform abnormally.	9.8	More Details
CVE-2022-48513	Vulnerability of identity verification being bypassed in the Gallery module. Successful exploitation of this vulnerability may cause out-of-bounds access.	9.8	More Details
CVE-2023-37242	Vulnerability of commands from the modem being intercepted in the atcmdserver module. Attackers may exploit this vulnerability to rewrite the non-volatile random-access memory (NVRAM), or facilitate the exploitation of other vulnerabilities.	9.8	More Details
CVE-2023-36993	The cryptographically insecure random number generator being used in TravianZ 8.3.4 and 8.3.3 in the password reset function allows an attacker to guess the password reset.parameters and to take over accounts.	9.8	More Details
CVE-2023-36188	An issue in langchain v.0.0.64 allows a remote attacker to execute arbitrary code via the PALChain parameter in the Python exec method.	9.8	More Details
CVE-2023-23902	A buffer overflow vulnerability exists in the uhttpd login functionality of Milesight UR32L v32.3.0.5. A specially crafted network request can lead to remote code execution. An attacker can send a network request to trigger this vulnerability.	9.8	More Details
CVE-2023-29381	An issue in Zimbra Collaboration (ZCS) v.8.8.15 and v.9.0 allows a remote attacker to escalate privileges and obtain sensitive information via the password and 2FA parameters.	9.8	More Details

CVE Number	Description	Base Score	Reference
CVE-2020-22336	An issue was discovered in pdfcrack 0.17 thru 0.18, allows attackers to execute arbitrary code via a stack overflow in the MD5 function.	9.8	More Details
CVE-2023-27845	SQL injection vulnerability found in PrestaShop lekerawen_ocs before v.1.4.1 allow a remote attacker to gain privileges via the KerawenHelper::setCartOperationInfo, and KerawenHelper::resetCheckoutSessionData components.	9.8	More Details
CVE-2023-29824	A use-after-free issue was discovered in Py_FindObjects() function in SciPy versions prior to 1.8.0. NOTE: the vendor and discoverer indicate that this is not a security issue.	9.8	More Details
CVE-2023-35987	PiiGAB M-Bus contains hard-coded credentials which it uses for authentication.	9.8	More Details
CVE-2023-37144	Tenda AC10 v15.03.06.26 was discovered to contain a command injection vulnerability via the mac parameter in the function formWriteFacMac.	9.8	More Details
CVE-2023-37145	TOTOLINK LR350 V9.3.5u.6369_B20220309 was discovered to contain a command injection vulnerability via the hostname parameter in the setOpModeCfg function.	9.8	More Details
CVE-2023-37146	TOTOLINK LR350 V9.3.5u.6369_B20220309 was discovered to contain a command injection vulnerability via the FileName parameter in the UploadFirmwareFile function.	9.8	More Details
CVE-2023-37149	TOTOLINK LR350 V9.3.5u.6369_B20220309 was discovered to contain a command injection vulnerability via the FileName parameter in the setUploadSetting function.	9.8	More Details
CVE-2023-37148	TOTOLINK LR350 V9.3.5u.6369_B20220309 was discovered to contain a command injection vulnerability via the ussd parameter in the setUssd function.	9.8	More Details
CVE-2023-24492	A vulnerability has been discovered in the Citrix Secure Access client for Ubuntu which, if exploited, could allow an attacker to remotely execute code if a victim user opens an attacker-crafted link and accepts further prompts.	9.6	More Details

CVE Number	Description	Base Score	Reference
CVE-2023-37277	XWiki Platform is a generic wiki platform offering runtime services for applications built on top of it. The REST API allows executing all actions via POST requests and accepts `text/plain`, `multipart/form-data` or `application/www-form-urlencoded` as content types which can be sent via regular HTML forms, thus allowing cross-site request forgery. With the interaction of a user with programming rights, this allows remote code execution through script macros and thus impacts the integrity, availability and confidentiality of the whole XWiki installation. For regular cookie-based authentication, the vulnerability is mitigated by SameSite cookie restrictions but as of March 2023, these are not enabled by default in Firefox and Safari. The vulnerability has been patched in XWiki 14.10.8 and 15.2 by requiring a CSRF token header for certain request types that are susceptible to CSRF attacks.	9.6	More Details
CVE-2023-36825	Orchid is a Laravel package that allows application development of back-office applications, admin/user panels, and dashboards. A vulnerability present starting in version 14.0.0-alpha4 and prior to version 14.5.0 is related to the deserialization of untrusted data from the `_state` query parameter, which can result in remote code execution. The issue has been addressed in version 14.5.0. Users are advised to upgrade their software to this version or any subsequent versions that include the patch. There are no known workarounds.	9.6	More Details
CVE-2023-33150	Microsoft Office Security Feature Bypass Vulnerability	9.6	More Details
CVE-2023-30319	Cross Site Scripting (XSS) vulnerability in username field in /src/chatbotapp/LoginServlet.java in wliang6 ChatEngine commit fded8e710ad59f816867ad47d7fc4862f6502f3e, allows attackers to execute arbitrary code.	9.6	More Details

CVE Number	Description	Base Score	Reference
CVE-2023-37261	OpenComputers is a Minecraft mod that adds programmable computers and robots to the game. This issue affects every version of OpenComputers with the Internet Card feature enabled; that is, OpenComputers 1.2.0 until 1.8.3 in their most common, default configurations. If the OpenComputers mod is installed as part of a Minecraft server hosted on a popular cloud hosting provider, such as AWS, GCP and Azure, those metadata services' API endpoints are not forbidden (aka "blacklisted") by default. As such, any player can gain access to sensitive information exposed via those metadata servers, potentially allowing them to pivot or privilege escalate into the hosting provider. In addition, IPv6 addresses are not correctly filtered at all, allowing broader access into the local IPv6 network. This can allow a player on a server using an OpenComputers computer to access parts of the private IPv4 address space, as well as the whole IPv6 address space, in order to retrieve sensitive information. OpenComputers v1.8.3 for Minecraft 1.7.10 and 1.12.2 contains a patch for this issue. Some workarounds are also available. One may disable the Internet Card feature completely. If using OpenComputers 1.3.0 or above, using the allow list (`opencomputers.internet.whitelist` option) will prohibit connections to any IP addresses and/or domains not listed; or one may add entries to the block list (`opencomputers.internet.blacklist` option). More information about mitigations is available in the GitHub Security Advisory.	9.6	More Details
CVE-2023-37262	CC: Tweaked is a mod for Minecraft which adds programmable computers, turtles, and more to the game. Prior to versions 1.20.1-1.106.0, 1.19.4-1.106.0, 1.19.2-1.101.3, 1.18.2-1.101.3, and 1.16.5-1.101.3, if the cc-tweaked plugin is running on a Minecraft server hosted on a popular cloud hosting providers, like AWS, GCP, and Azure, those metadata services API endpoints are not forbidden (aka "blacklisted") by default. As such, any player can gain access to sensitive information exposed via those metadata servers, potentially allowing them to pivot or privilege escalate into the hosting provider. Versions 1.20.1-1.106.0, 1.19.4-1.106.0, 1.19.2-1.101.3, 1.18.2-1.101.3, and 1.16.5-1.101.3 contain a fix for this issue.	9.6	More Details
CVE-2023-2746	The Rockwell Automation Enhanced HIM software contains an API that the application uses that is not protected sufficiently and uses incorrect Cross-Origin Resource Sharing (CORS) settings and, as a result, is vulnerable to a Cross Site Request Forgery (CSRF) attack. To exploit this vulnerability, a malicious user would have to convince a user to click on an untrusted link through a social engineering attack or successfully perform a Cross Site Scripting Attack (XSS). Exploitation of a CSRF could potentially lead to sensitive information disclosure and full remote access to the affected products.	9.6	More Details

CVE Number	Description	Base Score	Reference
CVE-2023-36459	Mastodon is a free, open-source social network server based on ActivityPub. Starting in version 1.3 and prior to versions 3.5.9, 4.0.5, and 4.1.3, an attacker using carefully crafted oEmbed data can bypass the HTML sanitization performed by Mastodon and include arbitrary HTML in oEmbed preview cards. This introduces a vector for cross-site scripting (XSS) payloads that can be rendered in the user's browser when a preview card for a malicious link is clicked through. Versions 3.5.9, 4.0.5, and 4.1.3 contain a patch for this issue.	9.3	More Details
CVE-2023-31191	DroneScout ds230 Remote ID receiver from BlueMark Innovations is affected by an information loss vulnerability through traffic injection. An attacker can exploit this vulnerability by injecting, on carefully selected channels, high power spoofed Open Drone ID (ODID) messages which force the DroneScout ds230 Remote ID receiver to drop real Remote ID (RID) information and, instead, generate and transmit JSON encoded MQTT messages containing crafted RID information. Consequently, the MQTT broker, typically operated by a system integrator, will have no access to the drones' real RID information. This issue affects the adjacent channel suppression algorithm present in DroneScout ds230 firmware from version 20211210-1627 through 20230329-1042.	9.3	More Details
CVE-2021-4406	An administrator is able to execute commands as root via the alerts management dialog	9.1	More Details
CVE-2023-36922	Due to programming error in function module and report, IS-OIL component in SAP ECC and SAP S/4HANA allows an authenticated attacker to inject an arbitrary operating system command into an unprotected parameter in a common (default) extension. On successful exploitation, the attacker can read or modify the system data as well as shut down the system.	9.1	More Details
CVE-2023-3455	Key management vulnerability on system. Successful exploitation of this vulnerability may affect service availability and integrity.	9.1	More Details
CVE-2023-36934	In Progress MOVEit Transfer before 2020.1.11 (12.1.11), 2021.0.9 (13.0.9), 2021.1.7 (13.1.7), 2022.0.7 (14.0.7), 2022.1.8 (14.1.8), and 2023.0.4 (15.0.4), a SQL injection vulnerability has been identified in the MOVEit Transfer web application that could allow an unauthenticated attacker to gain unauthorized access to the MOVEit Transfer database. An attacker could submit a crafted payload to a MOVEit Transfer application endpoint that could result in modification and disclosure of MOVEit database content.	9.1	More Details

CVE Number	Description	Base Score	Reference
CVE-2023-37245	Buffer overflow vulnerability in the modem pinctrl module. Successful exploitation of this vulnerability may affect the integrity and availability of the modem.	9.1	More Details
CVE-2023-37240	Vulnerability of missing input length verification in the distributed file system. Successful exploitation of this vulnerability may cause out-of-bounds read.	9.1	More Details
CVE-2023-37287	SmartBPM.NET has a vulnerability of using hard-coded authentication key. An unauthenticated remote attacker can exploit this vulnerability to access system with regular user privilege to read application data, and execute submission and approval processes.	9.1	More Details
CVE-2021-42081	An authenticated administrator is allowed to remotely execute arbitrary shell commands via the API.	9.1	More Details
CVE-2023-36755	A vulnerability has been identified in RUGGEDCOM ROX MX5000 (All versions < V2.16.0), RUGGEDCOM ROX MX5000RE (All versions < V2.16.0), RUGGEDCOM ROX RX1400 (All versions < V2.16.0), RUGGEDCOM ROX RX1500 (All versions < V2.16.0), RUGGEDCOM ROX RX1501 (All versions < V2.16.0), RUGGEDCOM ROX RX1510 (All versions < V2.16.0), RUGGEDCOM ROX RX1511 (All versions < V2.16.0), RUGGEDCOM ROX RX1512 (All versions < V2.16.0), RUGGEDCOM ROX RX1524 (All versions < V2.16.0), RUGGEDCOM ROX RX1536 (All versions < V2.16.0), RUGGEDCOM ROX RX5000 (All versions < V2.16.0). The SCEP CA Certificate Name parameter in the web interface of affected devices is vulnerable to command injection due to missing server side input sanitation. This could allow an authenticated privileged remote attacker to execute arbitrary code with root privileges.	9.1	More Details
CVE-2023-36754	A vulnerability has been identified in RUGGEDCOM ROX MX5000 (All versions < V2.16.0), RUGGEDCOM ROX MX5000RE (All versions < V2.16.0), RUGGEDCOM ROX RX1400 (All versions < V2.16.0), RUGGEDCOM ROX RX1500 (All versions < V2.16.0), RUGGEDCOM ROX RX1501 (All versions < V2.16.0), RUGGEDCOM ROX RX1510 (All versions < V2.16.0), RUGGEDCOM ROX RX1511 (All versions < V2.16.0), RUGGEDCOM ROX RX1512 (All versions < V2.16.0), RUGGEDCOM ROX RX1524 (All versions < V2.16.0), RUGGEDCOM ROX RX1536 (All versions < V2.16.0), RUGGEDCOM ROX RX5000 (All versions < V2.16.0). The SCEP server configuration URL parameter in the web interface of affected devices is vulnerable to command injection due to missing server side input sanitation. This could allow an authenticated privileged remote attacker to execute arbitrary code with root privileges.	9.1	More Details

CVE Number	Description	Base Score	Reference
CVE-2023-36753	A vulnerability has been identified in RUGGEDCOM ROX MX5000 (All versions < V2.16.0), RUGGEDCOM ROX MX5000RE (All versions < V2.16.0), RUGGEDCOM ROX RX1400 (All versions < V2.16.0), RUGGEDCOM ROX RX1500 (All versions < V2.16.0), RUGGEDCOM ROX RX1501 (All versions < V2.16.0), RUGGEDCOM ROX RX1510 (All versions < V2.16.0), RUGGEDCOM ROX RX1511 (All versions < V2.16.0), RUGGEDCOM ROX RX1512 (All versions < V2.16.0), RUGGEDCOM ROX RX1524 (All versions < V2.16.0), RUGGEDCOM ROX RX1536 (All versions < V2.16.0), RUGGEDCOM ROX RX5000 (All versions < V2.16.0). The uninstall-app App-name parameter in the web interface of affected devices is vulnerable to command injection due to missing server side input sanitation. This could allow an authenticated privileged remote attacker to execute arbitrary code with root privileges.	9.1	More Details
CVE-2023-36752	A vulnerability has been identified in RUGGEDCOM ROX MX5000 (All versions < V2.16.0), RUGGEDCOM ROX MX5000RE (All versions < V2.16.0), RUGGEDCOM ROX RX1400 (All versions < V2.16.0), RUGGEDCOM ROX RX1500 (All versions < V2.16.0), RUGGEDCOM ROX RX1501 (All versions < V2.16.0), RUGGEDCOM ROX RX1510 (All versions < V2.16.0), RUGGEDCOM ROX RX1511 (All versions < V2.16.0), RUGGEDCOM ROX RX1512 (All versions < V2.16.0), RUGGEDCOM ROX RX1524 (All versions < V2.16.0), RUGGEDCOM ROX RX1536 (All versions < V2.16.0), RUGGEDCOM ROX RX5000 (All versions < V2.16.0). The upgrade-app URL parameter in the web interface of affected devices is vulnerable to command injection due to missing server side input sanitation. This could allow an authenticated privileged remote attacker to execute arbitrary code with root privileges.	9.1	More Details
CVE-2023-36751	A vulnerability has been identified in RUGGEDCOM ROX MX5000 (All versions < V2.16.0), RUGGEDCOM ROX MX5000RE (All versions < V2.16.0), RUGGEDCOM ROX RX1400 (All versions < V2.16.0), RUGGEDCOM ROX RX1500 (All versions < V2.16.0), RUGGEDCOM ROX RX1501 (All versions < V2.16.0), RUGGEDCOM ROX RX1510 (All versions < V2.16.0), RUGGEDCOM ROX RX1511 (All versions < V2.16.0), RUGGEDCOM ROX RX1512 (All versions < V2.16.0), RUGGEDCOM ROX RX1524 (All versions < V2.16.0), RUGGEDCOM ROX RX1536 (All versions < V2.16.0), RUGGEDCOM ROX RX5000 (All versions < V2.16.0). The install-app URL parameter in the web interface of affected devices is vulnerable to command injection due to missing server side input sanitation. This could allow an authenticated privileged remote attacker to execute arbitrary code with root privileges.	9.1	More Details

CVE Number	Description	Base Score	Reference
CVE-2023-36750	A vulnerability has been identified in RUGGEDCOM ROX MX5000 (All versions < V2.16.0), RUGGEDCOM ROX MX5000RE (All versions < V2.16.0), RUGGEDCOM ROX RX1400 (All versions < V2.16.0), RUGGEDCOM ROX RX1500 (All versions < V2.16.0), RUGGEDCOM ROX RX1501 (All versions < V2.16.0), RUGGEDCOM ROX RX1510 (All versions < V2.16.0), RUGGEDCOM ROX RX1511 (All versions < V2.16.0), RUGGEDCOM ROX RX1512 (All versions < V2.16.0), RUGGEDCOM ROX RX1524 (All versions < V2.16.0), RUGGEDCOM ROX RX1536 (All versions < V2.16.0), RUGGEDCOM ROX RX5000 (All versions < V2.16.0). The software-upgrade Url parameter in the web interface of affected devices is vulnerable to command injection due to missing server side input sanitation. This could allow an authenticated privileged remote attacker to execute arbitrary code with root privileges.	9.1	More Details
CVE-2023-32250	A flaw was found in the Linux kernel's ksmbd, a high-performance in-kernel SMB server. The specific flaw exists within the processing of SMB2_SESSION_SETUP commands. The issue results from the lack of proper locking when performing operations on an object. An attacker can leverage this vulnerability to execute code in the context of the kernel.	9.0	More Details
CVE-2023-30320	Cross Site Scripting (XSS) vulnerability in textMessage field in /src/chatbotapp/chatWindow.java in wliang6 ChatEngine commit fded8e710ad59f816867ad47d7fc4862f6502f3e, allows attackers to execute arbitrary code.	9.0	More Details
CVE-2023-30321	Cross Site Scripting (XSS) vulnerability in textMessage field in /src/chatbotapp/LoginServlet.java in wliang6 ChatEngine commit fded8e710ad59f816867ad47d7fc4862f6502f3e, allows attackers to execute arbitrary code.	9.0	More Details
CVE-2023-34192	Cross Site Scripting vulnerability in Zimbra ZCS v.8.8.15 allows a remote authenticated attacker to execute arbitrary code via a crafted script to the /h/autoSaveDraft function.	9.0	More Details

OTHER VULNERABILITIES

CVE Number	Description	Base Score	Reference
CVE-2022-42175	Insecure Direct Object Reference vulnerability in WHMCS module SolusVM 1 4.1.2 allows an attacker to change the password and hostname of other customer servers without authorization.	8.8	More Details

CVE Number	Description	Base Score	Reference
CVE-2023-33159	Microsoft SharePoint Server Spoofing Vulnerability	8.8	More Details
CVE-2023-22299	An OS command injection vulnerability exists in the vtysh_ubus _get_fw_logs functionality of Milesight UR32L v32.3.0.5. A specially crafted network request can lead to command execution. An attacker can send a network request to trigger this vulnerability.	8.8	More Details
CVE-2020-21861	File upload vulnerability in DuxCMS 2.1 allows attackers to execute arbitrary php code via duxcms/AdminUpload/upload.	8.8	More Details
CVE-2023-3627	Cross-Site Request Forgery (CSRF) in GitHub repository salesagility/suitecrm-core prior to 8.3.1.	8.8	More Details
CVE-2023-32049	Windows SmartScreen Security Feature Bypass Vulnerability	8.8	More Details
CVE-2023-33134	Microsoft SharePoint Server Remote Code Execution Vulnerability	8.8	More Details
CVE-2023-33157	Microsoft SharePoint Remote Code Execution Vulnerability	8.8	More Details
CVE-2023-33160	Microsoft SharePoint Server Remote Code Execution Vulnerability	8.8	More Details
CVE-2023-2072	The Rockwell Automation PowerMonitor 1000 contains stored cross-site scripting vulnerabilities within the web page of the product. The vulnerable pages do not require privileges to access and can be injected with code by an attacker which could be used to leverage an attack on an authenticated user resulting in remote code execution and potentially the complete loss of confidentiality, integrity, and availability of the product.	8.8	More Details
CVE-2023-35300	Remote Procedure Call Runtime Remote Code Execution Vulnerability	8.8	More Details

CVE Number	Description	Base Score	Reference
CVE-2023-36821	Uptime Kuma, a self-hosted monitoring tool, allows an authenticated attacker to install a maliciously crafted plugin in versions prior to 1.22.1, which may lead to remote code execution. Uptime Kuma allows authenticated users to install plugins from an official list of plugins. This feature is currently disabled in the web interface, but the corresponding API endpoints are still available after login. After downloading a plugin, it's installed by calling `npm install` in the installation directory of the plugin. Because the plugin is not validated against the official list of plugins or installed with `npm install --ignore-scripts`, a maliciously crafted plugin taking advantage of npm scripts can gain remote code execution. Version 1.22.1 contains a patch for this issue.	8.8	More Details
CVE-2023-35302	Microsoft PostScript and PCL6 Class Printer Driver Remote Code Execution Vulnerability	8.8	More Details
CVE-2023-35303	USB Audio Class System Driver Remote Code Execution Vulnerability	8.8	More Details
CVE-2023-35311	Microsoft Outlook Security Feature Bypass Vulnerability	8.8	More Details
CVE-2023-35315	Windows Layer-2 Bridge Network Driver Remote Code Execution Vulnerability	8.8	More Details
CVE-2023-22653	An OS command injection vulnerability exists in the vtysh_ubus tcpdump_start_cb functionality of Milesight UR32L v32.3.0.5. A specially crafted HTTP request can lead to command execution. An authenticated attacker can send an HTTP request to trigger this vulnerability.	8.8	More Details
CVE-2023-24018	A stack-based buffer overflow vulnerability exists in the libzebra.so.0.0.0 security_decrypt_password functionality of Milesight UR32L v32.3.0.5. A specially crafted HTTP request can lead to a buffer overflow. An authenticated attacker can send an HTTP request to trigger this vulnerability.	8.8	More Details
CVE-2023-35333	MediaWiki PandocUpload Extension Remote Code Execution Vulnerability	8.8	More Details

CVE Number	Description	Base Score	Reference
CVE-2023-1597	The tagDiv Cloud Library WordPress plugin before 2.7 does not have authorisation and CSRF in an AJAX action accessible to both unauthenticated and authenticated users, allowing unauthenticated users to change arbitrary user metadata, which could lead to privilege escalation by setting themselves as an admin of the blog.	8.8	More Details
CVE-2023-34193	File Upload vulnerability in Zimbra ZCS 8.8.15 allows an authenticated privileged user to execute arbitrary code and obtain sensitive information via the ClientUploader function.	8.8	More Details
CVE-2023-36859	PiiGAB M-Bus SoftwarePack 900S does not correctly sanitize user input, which could allow an attacker to inject arbitrary commands.	8.8	More Details
CVE-2023-35120	PiiGAB M-Bus is vulnerable to cross-site request forgery. An attacker who wants to execute a certain command could send a phishing mail to the owner of the device and hope that the owner clicks on the link. If the owner of the device has a cookie stored that allows the owner to be logged in, then the device could execute the GET or POST link request.	8.8	More Details
CVE-2023-36969	CMS Made Simple v2.2.17 is vulnerable to Remote Command Execution via the File Upload Function.	8.8	More Details
CVE-2023-25201	Cross Site Request Forgery (CSRF) vulnerability in MultiTech Conduit AP MTCAP2-L4E1 MTCAP2-L4E1-868-042A v.6.0.0 allows a remote attacker to execute arbitrary code via a crafted script upload.	8.8	More Details
CVE-2023-33664	ai-dev aicombinationsonfly before v0.3.1 was discovered to contain a SQL injection vulnerability via the component /includes/ajax.php.	8.8	More Details
CVE-2023-30765	Delta Electronics InfraSuite Device Master versions prior to 1.0.7 contain improper access controls that could allow an attacker to alter privilege management configurations, resulting in privilege escalation.	8.8	More Details
CVE-2023-24519	Two OS command injection vulnerability exist in the vtysh_ubus toolsh_excute.constprop.1 functionality of Milesight UR32L v32.3.0.5. A specially-crafted network request can lead to command execution. An attacker can send a network request to trigger these vulnerabilities.This command injection is in the ping tool utility.	8.8	More Details

CVE Number	Description	Base Score	Reference
CVE-2023-36386	A vulnerability has been identified in RUGGEDCOM ROX MX5000 (All versions < V2.16.0), RUGGEDCOM ROX MX5000RE (All versions < V2.16.0), RUGGEDCOM ROX RX1400 (All versions < V2.16.0), RUGGEDCOM ROX RX1500 (All versions < V2.16.0), RUGGEDCOM ROX RX1501 (All versions < V2.16.0), RUGGEDCOM ROX RX1510 (All versions < V2.16.0), RUGGEDCOM ROX RX1511 (All versions < V2.16.0), RUGGEDCOM ROX RX1512 (All versions < V2.16.0), RUGGEDCOM ROX RX1524 (All versions < V2.16.0), RUGGEDCOM ROX RX1536 (All versions < V2.16.0), RUGGEDCOM ROX RX5000 (All versions < V2.16.0). A reflected cross-site scripting (XSS) vulnerability exists in the web interface of the affected application that could allow an attacker to execute malicious javascript code by tricking users into accessing a malicious link. The value is reflected in the response without sanitization while throwing an “invalid params element name” error on the get_elements parameters.	8.8	More Details
CVE-2023-36389	A vulnerability has been identified in RUGGEDCOM ROX MX5000 (All versions < V2.16.0), RUGGEDCOM ROX MX5000RE (All versions < V2.16.0), RUGGEDCOM ROX RX1400 (All versions < V2.16.0), RUGGEDCOM ROX RX1500 (All versions < V2.16.0), RUGGEDCOM ROX RX1501 (All versions < V2.16.0), RUGGEDCOM ROX RX1510 (All versions < V2.16.0), RUGGEDCOM ROX RX1511 (All versions < V2.16.0), RUGGEDCOM ROX RX1512 (All versions < V2.16.0), RUGGEDCOM ROX RX1524 (All versions < V2.16.0), RUGGEDCOM ROX RX1536 (All versions < V2.16.0), RUGGEDCOM ROX RX5000 (All versions < V2.16.0). A reflected cross-site scripting (XSS) vulnerability exists in the web interface of the affected application that could allow an attacker to execute malicious javascript code by tricking users into accessing a malicious link. The malformed value is reflected directly in the response without sanitization while throwing an “invalid path” error.	8.8	More Details

CVE Number	Description	Base Score	Reference
CVE-2023-36390	A vulnerability has been identified in RUGGEDCOM ROX MX5000 (All versions < V2.16.0), RUGGEDCOM ROX MX5000RE (All versions < V2.16.0), RUGGEDCOM ROX RX1400 (All versions < V2.16.0), RUGGEDCOM ROX RX1500 (All versions < V2.16.0), RUGGEDCOM ROX RX1501 (All versions < V2.16.0), RUGGEDCOM ROX RX1510 (All versions < V2.16.0), RUGGEDCOM ROX RX1511 (All versions < V2.16.0), RUGGEDCOM ROX RX1512 (All versions < V2.16.0), RUGGEDCOM ROX RX1524 (All versions < V2.16.0), RUGGEDCOM ROX RX1536 (All versions < V2.16.0), RUGGEDCOM ROX RX5000 (All versions < V2.16.0). A reflected cross-site scripting (XSS) vulnerability exists in the web interface of the affected application that could allow an attacker to execute malicious javascript code by tricking users into accessing a malicious link. The value is reflected in the response without sanitization while throwing an “invalid params element name” error on the action parameters.	8.8	More Details
CVE-2023-24583	Two OS command injection vulnerabilities exist in the urvpn_client cmd_name_action functionality of Milesight UR32L v32.3.0.5. A specially crafted network request can lead to arbitrary command execution. An attacker can send a network request to trigger these vulnerabilities.This OS command injection is triggered through a UDP packet.	8.8	More Details
CVE-2023-24582	Two OS command injection vulnerabilities exist in the urvpn_client cmd_name_action functionality of Milesight UR32L v32.3.0.5. A specially crafted network request can lead to arbitrary command execution. An attacker can send a network request to trigger these vulnerabilities.This OS command injection is triggered through a TCP packet.	8.8	More Details
CVE-2023-24520	Two OS command injection vulnerability exist in the vtysh_ubus toolsh_excute.constprop.1 functionality of Milesight UR32L v32.3.0.5. A specially-crafted network request can lead to command execution. An attacker can send a network request to trigger these vulnerabilities.This command injection is in the trace tool utility.	8.8	More Details
CVE-2023-35322	Windows Deployment Services Remote Code Execution Vulnerability	8.8	More Details
CVE-2023-32038	Microsoft ODBC Driver Remote Code Execution Vulnerability	8.8	More Details
CVE-2023-37201	An attacker could have triggered a use-after-free condition when creating a WebRTC connection over HTTPS. This vulnerability affects Firefox < 115, Firefox ESR < 102.13, and Thunderbird < 102.13.	8.8	More Details

CVE Number	Description	Base Score	Reference
CVE-2023-37202	Cross-compartment wrappers wrapping a scripted proxy could have caused objects from other compartments to be stored in the main compartment resulting in a use-after-free. This vulnerability affects Firefox < 115, Firefox ESR < 102.13, and Thunderbird < 102.13.	8.8	More Details
CVE-2023-35364	Windows Kernel Elevation of Privilege Vulnerability	8.8	More Details
CVE-2023-37212	Memory safety bugs present in Firefox 114. Some of these bugs showed evidence of memory corruption and we presume that with enough effort some of these could have been exploited to run arbitrary code. This vulnerability affects Firefox < 115.	8.8	More Details
CVE-2023-37211	Memory safety bugs present in Firefox 114, Firefox ESR 102.12, and Thunderbird 102.12. Some of these bugs showed evidence of memory corruption and we presume that with enough effort some of these could have been exploited to run arbitrary code. This vulnerability affects Firefox < 115, Firefox ESR < 102.13, and Thunderbird < 102.13.	8.8	More Details
CVE-2023-37209	A use-after-free condition existed in `NotifyOnHistoryReload` where a `LoadingSessionHistoryEntry` object was freed and a reference to that object remained. This resulted in a potentially exploitable condition when the reference to that object was later reused. This vulnerability affects Firefox < 115.	8.8	More Details
CVE-2023-35971	A vulnerability in the ArubaOS web-based management interface could allow an unauthenticated remote attacker to conduct a stored 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.	8.8	More Details
CVE-2023-29347	Windows Admin Center Spoofing Vulnerability	8.7	More Details
CVE-2021-42083	An authenticated attacker is able to create alerts that trigger a stored XSS attack.	8.7	More Details
CVE-2023-33989	An attacker with non-administrative authorizations in SAP NetWeaver (BI CONT ADD ON) - versions 707, 737, 747, 757, can exploit a directory traversal flaw to over-write system files. Data from confidential files cannot be read but potentially some OS files can be over-written leading to system compromise.	8.7	More Details

CVE Number	Description	Base Score	Reference
CVE-2023-36521	A vulnerability has been identified in SIMATIC MV540 H (All versions < V3.3.4), SIMATIC MV540 S (All versions < V3.3.4), SIMATIC MV550 H (All versions < V3.3.4), SIMATIC MV550 S (All versions < V3.3.4), SIMATIC MV560 U (All versions < V3.3.4), SIMATIC MV560 X (All versions < V3.3.4). The result synchronization server of the affected products contains a vulnerability that may lead to a denial of service condition. An attacker may cause a denial of service situation of all socket-based communication of the affected products if the result server is enabled.	8.6	More Details
CVE-2023-36808	GLPI is a free asset and IT management software package. Starting in version 0.80 and prior to version 10.0.8, Computer Virtual Machine form and GLPI inventory request can be used to perform a SQL injection attack. Version 10.0.8 has a patch for this issue. As a workaround, one may disable native inventory.	8.6	More Details
CVE-2023-35924	GLPI is a free asset and IT management software package. Starting in version 10.0.0 and prior to version 10.0.8, GLPI inventory endpoint can be used to drive a SQL injection attack. By default, GLPI inventory endpoint requires no authentication. Version 10.0.8 has a patch for this issue. As a workaround, one may disable native inventory.	8.6	More Details
CVE-2023-33987	An unauthenticated attacker in SAP Web Dispatcher - versions WEBDISP 7.49, WEBDISP 7.53, WEBDISP 7.54, WEBDISP 7.77, WEBDISP 7.81, WEBDISP 7.85, WEBDISP 7.88, WEBDISP 7.89, WEBDISP 7.90, KERNEL 7.49, KERNEL 7.53, KERNEL 7.54 KERNEL 7.77, KERNEL 7.81, KERNEL 7.85, KERNEL 7.88, KERNEL 7.89, KERNEL 7.90, KRNL64NUC 7.49, KRNL64UC 7.49, KRNL64UC 7.53, HDB 2.00, XS_ADVANCED_RUNTIME 1.00, SAP_EXTENDED_APP_SERVICES 1, can submit a malicious crafted request over a network to a front-end server which may, over several attempts, result in a back-end server confusing the boundaries of malicious and legitimate messages. This can result in the back-end server executing a malicious payload which can be used to read or modify information on the server or make it temporarily unavailable.	8.6	More Details
CVE-2023-3270	Exposure of Sensitive Information to an Unauthorized Actor in the SICK ICR890-4 could allow an unauthenticated remote attacker to retrieve sensitive information about the system.	8.6	More Details
CVE-2023-30664	Improper input validation vulnerability in RegisteredMSISDN prior to SMR Jul-2023 Release 1 allows local attackers to launch privileged activities.	8.5	More Details

CVE Number	Description	Base Score	Reference
CVE-2023-30658	Improper input validation vulnerability in DataProfile prior to SMR Jul-2023 Release 1 allows local attackers to launch privileged activities.	8.5	More Details
CVE-2023-30656	Improper input validation vulnerability in LSOItemData prior to SMR Jul-2023 Release 1 allows attackers to launch certain activities.	8.5	More Details
CVE-2023-30655	Improper input validation vulnerability in SCEPProfile prior to SMR Jul-2023 Release 1 allows local attackers to launch privileged activities.	8.5	More Details
CVE-2023-37271	RestrictedPython is a tool that helps to define a subset of the Python language which allows users to provide a program input into a trusted environment. RestrictedPython does not check access to stack frames and their attributes. Stack frames are accessible within at least generators and generator expressions, which are allowed inside RestrictedPython. Prior to versions 6.1 and 5.3, an attacker with access to a RestrictedPython environment can write code that gets the current stack frame in a generator and then walk the stack all the way beyond the RestrictedPython invocation boundary, thus breaking out of the restricted sandbox and potentially allowing arbitrary code execution in the Python interpreter. All RestrictedPython deployments that allow untrusted users to write Python code in the RestrictedPython environment are at risk. In terms of Zope and Plone, this would mean deployments where the administrator allows untrusted users to create and/or edit objects of type `Script (Python)`, `DTML Method`, `DTML Document` or `Zope Page Template`. This is a non-default configuration and likely to be extremely rare. The problem has been fixed in versions 6.1 and 5.3.	8.4	More Details
CVE-2023-30431	IBM Db2 for Linux, UNIX and Windows (includes Db2 Connect Server) 10.5, 11.1, and 11.5 db2set is vulnerable to a buffer overflow, caused by improper bounds checking. An attacker could overflow the buffer and execute arbitrary code. IBM X-Force ID: 252184.	8.4	More Details
CVE-2023-27558	IBM Db2 on Windows 10.5, 11.1, and 11.5 may be vulnerable to a privilege escalation caused by at least one installed service using an unquoted service path. A local attacker could exploit this vulnerability to gain elevated privileges by inserting an executable file in the path of the affected service. IBM X-Force ID: 249194.	8.4	More Details
CVE-2023-36538	Improper access control in Zoom Rooms for Windows before version 5.15.0 may allow an authenticated user to enable an escalation of privilege via local access.	8.4	More Details

CVE Number	Description	Base Score	Reference
CVE-2023-36456	authentik is an open-source Identity Provider. Prior to versions 2023.4.3 and 2023.5.5, authentik does not verify the source of the X-Forwarded-For and X-Real-IP headers, both in the Python code and the go code. Only authentik setups that are directly accessible by users without a reverse proxy are susceptible to this. Possible spoofing of IP addresses in logs, downstream applications proxied by (built in) outpost, IP bypassing in custom flows if used. This poses a possible security risk when someone has flows or policies that check the user's IP address, e.g. when they want to ignore the user's 2 factor authentication when the user is connected to the company network. A second security risk is that the IP addresses in the logfiles and user sessions are not reliable anymore. Anybody can spoof this address and one cannot verify that the user has logged in from the IP address that is in their account's log. A third risk is that this header is passed on to the proxied application behind an outpost. The application may do any kind of verification, logging, blocking or rate limiting based on the IP address, and this IP address can be overridden by anybody that want to. Versions 2023.4.3 and 2023.5.5 contain a patch for this issue.	8.3	More Details
CVE-2023-2079	The "Buy Me a Coffee – Button and Widget Plugin" plugin for WordPress is vulnerable to Cross-Site Request Forgery due to missing nonce validation on the recieve_post, bmc_disconnect, name_post, and widget_post functions in versions up to, and including, 3.7. This makes it possible for unauthenticated attackers to update the plugins settings, via a forged request granted the attacker can trick a site's administrator into performing an action such as clicking on a link.	8.3	More Details
CVE-2023-36536	Untrusted search path in the installer for Zoom Rooms for Windows before version 5.15.0 may allow an authenticated user to enable an escalation of privilege via local access.	8.2	More Details
CVE-2023-37260	league/oauth2-server is an implementation of an OAuth 2.0 authorization server written in PHP. Starting in version 8.3.2 and prior to version 8.5.3, servers that passed their keys to the CryptKey constructor as as string instead of a file path will have had that key included in a LogicException message if they did not provide a valid pass phrase for the key where required. This issue has been patched so that the provided key is no longer exposed in the exception message in the scenario outlined above. Users should upgrade to version 8.5.3 to receive the patch. As a workaround, pass the key as a file instead of a string.	8.2	More Details
CVE-2023-34119	Insecure temporary file in the installer for Zoom Rooms for Windows before version 5.15.0 may allow an authenticated user to enable an escalation of privilege via local access.	8.2	More Details

CVE Number	Description	Base Score	Reference
CVE-2023-35335	Microsoft Dynamics 365 (on-premises) Cross-site Scripting Vulnerability	8.2	More Details
CVE-2023-3271	Improper Access Control in the SICK ICR890-4 could allow an unauthenticated remote attacker to gather information about the system and download data via the REST API by accessing unauthenticated endpoints.	8.2	More Details
CVE-2023-34116	Improper input validation in the Zoom Desktop Client for Windows before version 5.15.0 may allow an unauthorized user to enable an escalation of privilege via network access.	8.2	More Details
CVE-2023-33171	Microsoft Dynamics 365 (on-premises) Cross-site Scripting Vulnerability	8.2	More Details
CVE-2023-24019	A stack-based buffer overflow vulnerability exists in the urvpn_client http_connection_readcb functionality of Milesight UR32L v32.3.0.5. A specially crafted network packet can lead to a buffer overflow. An attacker can send a malicious packet to trigger this vulnerability.	8.1	More Details
CVE-2023-34089	Decidim is a participatory democracy framework, written in Ruby on Rails, originally developed for the Barcelona City government online and offline participation website. The processes filter feature is susceptible to Cross-site scripting. This allows a remote attacker to execute JavaScript code in the context of a currently logged-in user. An attacker could use this vulnerability to make other users endorse or support proposals they have no intention of supporting or endorsing. The problem was patched in version 0.27.3 and 0.26.7.	8.1	More Details
CVE-2023-33127	.NET and Visual Studio Elevation of Privilege Vulnerability	8.1	More Details

CVE Number	Description	Base Score	Reference
CVE-2023-31190	DroneScout ds230 Remote ID receiver from BlueMark Innovations is affected by an Improper Authentication vulnerability during the firmware update procedure. Specifically, the firmware update procedure ignores and does not check the validity of the TLS certificate of the HTTPS endpoint from which the firmware update package (.tar.bz2 file) is downloaded. An attacker with the ability to put himself in a Man-in-the-Middle situation (e.g., DNS poisoning, ARP poisoning, control of a node on the route to the endpoint, etc.) can trick the DroneScout ds230 to install a crafted malicious firmware update containing arbitrary files (e.g., executable and configuration) and gain administrative (root) privileges on the underlying Linux operating system. This issue affects DroneScout ds230 firmware from version 20211210-1627 through 20230329-1042.	8.1	More Details
CVE-2023-36690	Cross-Site Request Forgery (CSRF) vulnerability in VibeThemes WPLMS theme <= 4.900 versions.	8.1	More Details
CVE-2023-22371	An os command injection vulnerability exists in the liburvpn.so create_private_key functionality of Milesight VPN v2.0.2. A specially-crafted network request can lead to command execution. An attacker can send a malicious packet to trigger this vulnerability.	8.1	More Details
CVE-2023-37596	Cross Site Request Forgery (CSRF) vulnerability in issabel-pbx v.4.0.0-6 allows a remote attacker to cause a denial of service via a crafted script to the deleteuser function.	8.1	More Details
CVE-2023-33170	ASP.NET and Visual Studio Security Feature Bypass Vulnerability	8.1	More Details
CVE-2020-21862	Directory traversal vulnerability in DuxCMS 2.1 allows attackers to delete arbitrary files via /admin/AdminBackup/del.	8.1	More Details
CVE-2023-32693	Decidim is a participatory democracy framework, written in Ruby on Rails, originally developed for the Barcelona City government online and offline participation website. The external link feature is susceptible to cross-site scripting. This allows a remote attacker to execute JavaScript code in the context of a currently logged-in user. An attacker could use this vulnerability to make other users endorse or support proposals they have no intention of supporting or endorsing. The problem was patched in versions 0.27.3 and 0.26.7.	8.1	More Details

CVE Number	Description	Base Score	Reference
CVE-2023-37597	Cross Site Request Forgery (CSRF) vulnerability in issabel-pbx v.4.0.0-6 allows a remote attacker to cause a denial of service via the delete user grouplist function.	8.1	More Details
CVE-2023-36809	Kiwi TCMS, an open source test management system allows users to upload attachments to test plans, test cases, etc. Versions of Kiwi TCMS prior to 12.5 had introduced changes which were meant to serve all uploaded files as plain text in order to prevent browsers from executing potentially dangerous files when such files are accessed directly. The previous Nginx configuration was incorrect allowing certain browsers like Firefox to ignore the `Content-Type: text/plain` header on some occasions thus allowing potentially dangerous scripts to be executed. Additionally, file upload validators and parts of the HTML rendering code had been found to require additional sanitation and improvements. Version 12.5 fixes this vulnerability with updated Nginx content type configuration, improved file upload validation code to prevent more potentially dangerous uploads, and Sanitization of test plan names used in the `tree_view_html()` function.	8.1	More Details
CVE-2023-35297	Windows Pragmatic General Multicast (PGM) Remote Code Execution Vulnerability	8.1	More Details
CVE-2023-36932	In Progress MOVEit Transfer before 2020.1.11 (12.1.11), 2021.0.9 (13.0.9), 2021.1.7 (13.1.7), 2022.0.7 (14.0.7), 2022.1.8 (14.1.8), and 2023.0.4 (15.0.4), multiple SQL injection vulnerabilities have been identified in the MOVEit Transfer web application that could allow an authenticated attacker to gain unauthorized access to the MOVEit Transfer database. An attacker could submit a crafted payload to a MOVEit Transfer application endpoint that could result in modification and disclosure of MOVEit database content.	8.1	More Details
CVE-2023-35939	GLPI is a free asset and IT management software package. Starting in version 9.5.0 and prior to version 10.0.8, an incorrect rights check on a on a file accessible by an authenticated user (or not for certain actions), allows a threat actor to interact, modify, or see Dashboard data. Version 10.0.8 contains a patch for this issue.	8.1	More Details
CVE-2023-32652	PiiGAB M-Bus does not validate identification strings before processing, which could make it vulnerable to cross-site scripting attacks.	8.0	More Details
CVE-2023-35328	Windows Transaction Manager Elevation of Privilege Vulnerability	7.8	More Details

CVE Number	Description	Base Score	Reference
CVE-2023-36623	The root password of the Loxone Miniserver Go Gen.2 before 14.2 is calculated using hard-coded secrets and the MAC address. This allows a local user to calculate the root password and escalate privileges.	7.8	More Details
CVE-2023-37246	A vulnerability has been identified in Tecnomatix Plant Simulation V2201 (All versions < V2201.0008), Tecnomatix Plant Simulation V2302 (All versions < V2302.0002). The affected application is vulnerable to heap-based buffer overflow while parsing specially crafted PRT files. This could allow an attacker to execute code in the context of the current process. (ZDI-CAN-21109)	7.8	More Details
CVE-2023-21756	Windows Win32k Elevation of Privilege Vulnerability	7.8	More Details
CVE-2023-37247	A vulnerability has been identified in Tecnomatix Plant Simulation V2201 (All versions < V2201.0008), Tecnomatix Plant Simulation V2302 (All versions < V2302.0002). The affected application is vulnerable to heap-based buffer overflow while parsing specially crafted PAR files. This could allow an attacker to execute code in the context of the current process. (ZDI-CAN-21138)	7.8	More Details
CVE-2023-37248	A vulnerability has been identified in Tecnomatix Plant Simulation V2201 (All versions < V2201.0008), Tecnomatix Plant Simulation V2302 (All versions < V2302.0002). The affected application contains an out of bounds write past the end of an allocated buffer while parsing a specially crafted PAR file. This could allow an attacker to execute code in the context of the current process. (ZDI-CAN-21155)	7.8	More Details
CVE-2023-32183	Incorrect Default Permissions vulnerability in the openSUSE Tumbleweed hawk2 package allows users with access to the hacluster to escalate to root This issue affects openSUSE Tumbleweed.	7.8	More Details
CVE-2023-37374	A vulnerability has been identified in Tecnomatix Plant Simulation V2201 (All versions < V2201.0008), Tecnomatix Plant Simulation V2302 (All versions < V2302.0002). The affected application is vulnerable to stack-based buffer overflow while parsing specially crafted STP files. This could allow an attacker to execute code in the context of the current process. (ZDI-CAN-21054)	7.8	More Details
CVE-2023-35304	Windows Kernel Elevation of Privilege Vulnerability	7.8	More Details

CVE Number	Description	Base Score	Reference
CVE-2023-35317	Windows Server Update Service (WSUS) Elevation of Privilege Vulnerability	7.8	More Details
CVE-2023-37208	When opening Diagcab files, Firefox did not warn the user that these files may contain malicious code. This vulnerability affects Firefox < 115, Firefox ESR < 102.13, and Thunderbird < 102.13.	7.8	More Details
CVE-2023-36867	Visual Studio Code GitHub Pull Requests and Issues Extension Remote Code Execution Vulnerability	7.8	More Details
CVE-2023-35343	Windows Geolocation Service Remote Code Execution Vulnerability	7.8	More Details
CVE-2023-37203	Insufficient validation in the Drag and Drop API in conjunction with social engineering, may have allowed an attacker to trick end-users into creating a shortcut to local system files. This could have been leveraged to execute arbitrary code. This vulnerability affects Firefox < 115.	7.8	More Details
CVE-2023-35313	Windows Online Certificate Status Protocol (OCSP) SnapIn Remote Code Execution Vulnerability	7.8	More Details
CVE-2023-37375	A vulnerability has been identified in Tecnomatix Plant Simulation V2201 (All versions < V2201.0008), Tecnomatix Plant Simulation V2302 (All versions < V2302.0002). The affected application is vulnerable to stack-based buffer overflow while parsing specially crafted SPP files. This could allow an attacker to execute code in the context of the current process. (ZDI-CAN-21060)	7.8	More Details
CVE-2021-42082	Local users are able to execute scripts under root privileges.	7.8	More Details
CVE-2023-35337	Win32k Elevation of Privilege Vulnerability	7.8	More Details
CVE-2023-34432	A heap buffer overflow vulnerability was found in sox, in the lsx_readbuf function at sox/src/formats_i.c:98:16. This flaw can lead to a denial of service, code execution, or information disclosure.	7.8	More Details
CVE-2023-35340	Windows CNG Key Isolation Service Elevation of Privilege Vulnerability	7.8	More Details

CVE Number	Description	Base Score	Reference
CVE-2023-31248	Linux Kernel nftables Use-After-Free Local Privilege Escalation Vulnerability; `nft_chain_lookup_byid()` failed to check whether a chain was active and CAP_NET_ADMIN is in any user or network namespace	7.8	More Details
CVE-2023-35374	Paint 3D Remote Code Execution Vulnerability	7.8	More Details
CVE-2023-36624	Loxone Miniserver Go Gen.2 through 14.0.3.28 allows an authenticated operating system user to escalate privileges via the Sudo configuration. This allows the elevated execution of binaries without a password requirement.	7.8	More Details
CVE-2023-35312	Microsoft VOLSNAP.SYS Elevation of Privilege Vulnerability	7.8	More Details
CVE-2023-27390	A heap-based buffer overflow vulnerability exists in the Sequence::DrawText functionality of Diagon v1.0.139. A specially crafted markdown file can lead to arbitrary code execution. A victim would need to open a malicious file to trigger this vulnerability.	7.8	More Details
CVE-2023-35001	Linux Kernel nftables Out-Of-Bounds Read/Write Vulnerability; nft_byteorder poorly handled vm register contents when CAP_NET_ADMIN is in any user or network namespace	7.8	More Details
CVE-2023-35305	Windows Kernel Elevation of Privilege Vulnerability	7.8	More Details
CVE-2023-3269	A vulnerability exists in the memory management subsystem of the Linux kernel. The lock handling for accessing and updating virtual memory areas (VMAs) is incorrect, leading to use-after-free problems. This issue can be successfully exploited to execute arbitrary kernel code, escalate containers, and gain root privileges.	7.8	More Details
CVE-2023-34318	A heap buffer overflow vulnerability was found in sox, in the startread function at sox/src/hcom.c:160:41. This flaw can lead to a denial of service, code execution, or information disclosure.	7.8	More Details
CVE-2023-37376	A vulnerability has been identified in Tecnomatix Plant Simulation V2201 (All versions < V2201.0008), Tecnomatix Plant Simulation V2302 (All versions < V2302.0002). The affected application contains a type confusion vulnerability while parsing STP files. This could allow an attacker to execute code in the context of the current process. (ZDI-CAN-21051)	7.8	More Details

CVE Number	Description	Base Score	Reference
CVE-2023-35342	Windows Image Acquisition Elevation of Privilege Vulnerability	7.8	More Details
CVE-2023-33990	SAP SQL Anywhere - version 17.0, allows an attacker to prevent legitimate users from accessing the service by crashing the service. An attacker with low privileged account and access to the local system can write into the shared memory objects. This can be leveraged by an attacker to perform a Denial of Service. Further, an attacker might be able to modify sensitive data in shared memory objects.This issue only affects SAP SQL Anywhere on Windows. Other platforms are not impacted.	7.8	More Details
CVE-2023-33155	Windows Cloud Files Mini Filter Driver Elevation of Privilege Vulnerability	7.8	More Details
CVE-2023-30644	Stack out of bound write vulnerability in CdmaSmsParser of RILD prior to SMR Jul-2023 Release 1 allows attackers to execute arbitrary code.	7.8	More Details
CVE-2023-30645	Heap out of bound write vulnerability in IpcRxIncomingCBMsg of RILD prior to SMR Jul-2023 Release 1 allows attackers to execute arbitrary code.	7.8	More Details
CVE-2023-30646	Heap out of bound write vulnerability in BroadcastSmsConfig of RILD prior to SMR Jul-2023 Release 1 allows attackers to execute arbitrary code.	7.8	More Details
CVE-2023-30647	Heap out of bound write vulnerability in IpcRxUsimPhoneBookCapa of RILD prior to SMR Jul-2023 Release 1 allows attackers to execute arbitrary code.	7.8	More Details
CVE-2023-30649	Heap out of bound write vulnerability in RmtUimNeedApdu of RILD prior to SMR Jul-2023 Release 1 allows attackers to execute arbitrary code.	7.8	More Details
CVE-2023-35323	Windows OLE Remote Code Execution Vulnerability	7.8	More Details
CVE-2023-33161	Microsoft Excel Remote Code Execution Vulnerability	7.8	More Details
CVE-2023-35357	Windows Kernel Elevation of Privilege Vulnerability	7.8	More Details

CVE Number	Description	Base Score	Reference
CVE-2023-35358	Windows Kernel Elevation of Privilege Vulnerability	7.8	More Details
CVE-2023-24256	An issue in the com.nextev.datastatistic component of NIO EC6 Aspen before v3.3.0 allows attackers to escalate privileges via path traversal.	7.8	More Details
CVE-2023-33158	Microsoft Excel Remote Code Execution Vulnerability	7.8	More Details
CVE-2023-32046	Windows MSHTML Platform Elevation of Privilege Vulnerability	7.8	More Details
CVE-2023-35362	Windows Clip Service Elevation of Privilege Vulnerability	7.8	More Details
CVE-2023-35299	Windows Common Log File System Driver Elevation of Privilege Vulnerability	7.8	More Details
CVE-2023-33154	Windows Partition Management Driver Elevation of Privilege Vulnerability	7.8	More Details
CVE-2023-35353	Connected User Experiences and Telemetry Elevation of Privilege Vulnerability	7.8	More Details
CVE-2023-32047	Paint 3D Remote Code Execution Vulnerability	7.8	More Details
CVE-2023-24491	A vulnerability has been discovered in the Citrix Secure Access client for Windows which, if exploited, could allow an attacker with access to an endpoint with Standard User Account that has the vulnerable client installed to escalate their local privileges to that of NT AUTHORITY\SYSTEM.	7.8	More Details
CVE-2023-32051	Raw Image Extension Remote Code Execution Vulnerability	7.8	More Details

CVE Number	Description	Base Score	Reference
CVE-2023-32053	Windows Installer Elevation of Privilege Vulnerability	7.8	More Details
CVE-2023-35320	Connected User Experiences and Telemetry Elevation of Privilege Vulnerability	7.8	More Details
CVE-2023-32056	Windows Server Update Service (WSUS) Elevation of Privilege Vulnerability	7.8	More Details
CVE-2023-33149	Microsoft Office Graphics Remote Code Execution Vulnerability	7.8	More Details
CVE-2023-36874	Windows Error Reporting Service Elevation of Privilege Vulnerability	7.8	More Details
CVE-2023-35356	Windows Kernel Elevation of Privilege Vulnerability	7.8	More Details
CVE-2023-35363	Windows Kernel Elevation of Privilege Vulnerability	7.8	More Details
CVE-2023-33148	Microsoft Office Elevation of Privilege Vulnerability	7.8	More Details
CVE-2023-35871	The SAP Web Dispatcher - versions WEBDISP 7.53, WEBDISP 7.54, WEBDISP 7.77, WEBDISP 7.85, WEBDISP 7.89, WEBDISP 7.91, WEBDISP 7.92, WEBDISP 7.93, KERNEL 7.53, KERNEL 7.54 KERNEL 7.77, KERNEL 7.85, KERNEL 7.89, KERNEL 7.91, KERNEL 7.92, KERNEL 7.93, KRNL64UC 7.53, HDB 2.00, XS_ADVANCED_RUNTIME 1.00, SAP_EXTENDED_APP_SERVICES 1, has a vulnerability that can be exploited by an unauthenticated attacker to cause memory corruption through logical errors in memory management this may leads to information disclosure or system crashes, which can have low impact on confidentiality and high impact on the integrity and availability of the system.	7.7	More Details

CVE Number	Description	Base Score	Reference
CVE-2023-30643	Missing authentication vulnerability in Galaxy Themes Service prior to SMR Jul-2023 Release 1 allows local attackers to delete arbitrary non-preloaded applications.	7.7	More Details
CVE-2023-22835	A security defect was identified that enabled a user of Foundry Issues to perform a Denial of Service attack by submitting malformed data in an Issue that caused loss of frontend functionality to all issue participants. This defect was resolved with the release of Foundry Issues 2.510.0 and Foundry Frontend 6.228.0.	7.7	More Details
CVE-2023-34337	AMI SPx contains a vulnerability in the BMC where a user may cause an inadequate encryption strength by hash-based message authentication code (HMAC). A successful exploit of this vulnerability may lead to a loss of confidentiality, integrity, and availability.	7.6	More Details
CVE-2023-29095	Auth. (admin+) SQL Injection (SQLi) vulnerability in David F. Carr RSVPMaker plugin < 10.5.5 versions.	7.6	More Details
CVE-2023-37270	Piwigo is open source photo gallery software. Prior to version 13.8.0, there is a SQL Injection vulnerability in the login of the administrator screen. The SQL statement that acquires the HTTP Header `User-Agent` is vulnerable at the endpoint that records user information when logging in to the administrator screen. It is possible to execute arbitrary SQL statements. Someone who wants to exploit the vulnerability must be log in to the administrator screen, even with low privileges. Any SQL statement can be executed. Doing so may leak information from the database. Version 13.8.0 contains a fix for this issue. As another mitigation, those who want to execute a SQL statement verbatim with user-enterable parameters should be sure to escape the parameter contents appropriately.	7.6	More Details
CVE-2023-35325	Windows Print Spooler Information Disclosure Vulnerability	7.5	More Details
CVE-2023-36201	An issue in JerryscriptProject jerryscript v.3.0.0 allows an attacker to obtain sensitive information via a crafted script to the arrays.	7.5	More Details
CVE-2023-3273	Improper Access Control in the SICK ICR890-4 could allow an unauthenticated remote attacker to affect the availability of the device by changing settings of the device such as the IP address based on missing access control.	7.5	More Details

CVE Number	Description	Base Score	Reference
CVE-2023-3272	Cleartext Transmission of Sensitive Information in the SICK ICR890-4 could allow a remote attacker to gather sensitive information by intercepting network traffic that is not encrypted.	7.5	More Details
CVE-2023-36461	Mastodon is a free, open-source social network server based on ActivityPub. When performing outgoing HTTP queries, Mastodon sets a timeout on individual read operations. Prior to versions 3.5.9, 4.0.5, and 4.1.3, a malicious server can indefinitely extend the duration of the response through slowloris-type attacks. This vulnerability can be used to keep all Mastodon workers busy for an extended duration of time, leading to the server becoming unresponsive. Versions 3.5.9, 4.0.5, and 4.1.3 contain a patch for this issue.	7.5	More Details
CVE-2023-3127	An unauthenticated user could log into iSTAR Ultra, iSTAR Ultra LT, iSTAR Ultra G2, and iSTAR Edge G2 with administrator rights.	7.5	More Details
CVE-2023-30195	In the module "Detailed Order" (lgdetailedorder) in version up to 1.1.20 from Linea Grafica for PrestaShop, a guest can download personal informations without restriction formatted in json.	7.5	More Details
CVE-2023-20899	VMware SD-WAN (Edge) contains a bypass authentication vulnerability. An unauthenticated attacker can download the Diagnostic bundle of the application under VMware SD-WAN Management.	7.5	More Details
CVE-2023-31277	PiiGAB M-Bus transmits credentials in plaintext format.	7.5	More Details
CVE-2023-34433	PiiGAB M-Bus stores passwords using a weak hash algorithm.	7.5	More Details
CVE-2023-34995	There are no requirements for setting a complex password for PiiGAB M-Bus, which could contribute to a successful brute force attack if the password is inline with recommended password guidelines.	7.5	More Details
CVE-2023-35339	Windows CryptoAPI Denial of Service Vulnerability	7.5	More Details
CVE-2023-37192	Memory management and protection issues in Bitcoin Core v22 allows attackers to modify the stored sending address within the app's memory, potentially allowing them to redirect Bitcoin transactions to wallets of their own choosing.	7.5	More Details

CVE Number	Description	Base Score	Reference
CVE-2023-35338	Windows Peer Name Resolution Protocol Denial of Service Vulnerability	7.5	More Details
CVE-2023-29984	Null pointer dereference vulnerability exists in multiple vendors MFPs and printers which implement Debut web server 1.2 or 1.3. Processing a specially crafted request may lead an affected product to a denial-of-service (DoS) condition. As for the affected products/models/versions, see the detailed information provided by each vendor.	7.5	More Details
CVE-2023-30325	SQL Injection vulnerability in textMessage parameter in /src/chatbotapp/chatWindow.java in wliang6 ChatEngine v.1.0, allows attackers to gain sensitive information.	7.5	More Details
CVE-2023-30323	SQL Injection vulnerability in username field in /src/chatbotapp/chatWindow.java in Payatu ChatEngine v.1.0, allows attackers to gain sensitive information.	7.5	More Details
CVE-2022-31810	A vulnerability has been identified in SiPass integrated (All versions < V2.90.3.8). Affected server applications improperly check the size of data packets received for the configuration client login, causing a stack-based buffer overflow. This could allow an unauthenticated remote attacker to crash the server application, creating a denial of service condition.	7.5	More Details
CVE-2023-3553	Exposure of Sensitive Information to an Unauthorized Actor in GitHub repository nilsteampassnet/teampass prior to 3.0.10.	7.5	More Details
CVE-2023-2880	Frauscher Sensortechnik GmbH FDS001 for FAdC/FAdCi v1.3.3 and all previous versions are vulnerable to a path traversal vulnerability of the web interface by a crafted URL without authentication. This enables an remote attacker to read all files on the filesystem of the FDS001 device.	7.5	More Details
CVE-2023-30445	IBM Db2 for Linux, UNIX and Windows (includes Db2 Connect Server) 10.5, 11.1, and 11.5 is vulnerable to denial of service with a specially crafted query on certain tables. IBM X-Force ID: 253357.	7.5	More Details
CVE-2023-30449	IBM Db2 for Linux, UNIX and Windows (includes Db2 Connect Server) 10.5, 11.1, and 11.5 is vulnerable to denial of service with a specially crafted query. IBM X-Force ID: 253439.	7.5	More Details
CVE-2023-35696	Unauthenticated endpoints in the SICK ICR890-4 could allow an unauthenticated remote attacker to retrieve sensitive information about the device via HTTP requests.	7.5	More Details

CVE Number	Description	Base Score	Reference
CVE-2023-36933	In Progress MOVEit Transfer before 2021.0.9 (13.0.9), 2021.1.7 (13.1.7), 2022.0.7 (14.0.7), 2022.1.8 (14.1.8), and 2023.0.4 (15.0.4), it is possible for an attacker to invoke a method that results in an unhandled exception. Triggering this workflow can cause the MOVEit Transfer application to terminate unexpectedly.	7.5	More Details
CVE-2023-35330	Windows Extended Negotiation Denial of Service Vulnerability	7.5	More Details
CVE-2022-29561	A vulnerability has been identified in RUGGEDCOM ROX MX5000 (All versions < V2.16.0), RUGGEDCOM ROX MX5000RE (All versions < V2.16.0), RUGGEDCOM ROX RX1400 (All versions < V2.16.0), RUGGEDCOM ROX RX1500 (All versions < V2.16.0), RUGGEDCOM ROX RX1501 (All versions < V2.16.0), RUGGEDCOM ROX RX1510 (All versions < V2.16.0), RUGGEDCOM ROX RX1511 (All versions < V2.16.0), RUGGEDCOM ROX RX1512 (All versions < V2.16.0), RUGGEDCOM ROX RX1524 (All versions < V2.16.0), RUGGEDCOM ROX RX1536 (All versions < V2.16.0), RUGGEDCOM ROX RX5000 (All versions < V2.16.0). The web interface of the affected devices are vulnerable to Cross-Site Request Forgery attacks. By tricking an authenticated victim user to click a malicious link, an attacker could perform arbitrary actions on the device on behalf of the victim user.	7.5	More Details
CVE-2023-34090	Decidim is a participatory democracy framework, written in Ruby on Rails, originally developed for the Barcelona City government online and offline participation website. Decidim uses a third-party library named Ransack for filtering certain database collections (e.g., public meetings). By default, this library allows filtering on all data attributes and associations. This allows an unauthenticated remote attacker to exfiltrate non-public data from the underlying database of a Decidim instance (e.g., exfiltrating data from the user table). This issue may lead to Sensitive Data Disclosure. The problem was patched in version 0.27.3.	7.5	More Details
CVE-2023-23571	An access violation vulnerability exists in the eventcore functionality of Milesight UR32L v32.3.0.5. A specially crafted network request can lead to denial of service. An attacker can send a network request to trigger this vulnerability.	7.5	More Details
CVE-2022-48517	Unauthorized service access vulnerability in the DSoftBus module. Successful exploitation of this vulnerability will affect availability.	7.5	More Details

CVE Number	Description	Base Score	Reference
CVE-2023-36189	SQL injection vulnerability in langchain before v0.0.247 allows a remote attacker to obtain sensitive information via the SQLDatabaseChain component.	7.5	More Details
CVE-2022-48508	Inappropriate authorization vulnerability in the system apps. Successful exploitation of this vulnerability may affect service integrity.	7.5	More Details
CVE-2021-46896	Buffer Overflow vulnerability in PX4-Autopilot allows attackers to cause a denial of service via handler function handling msgid 332.	7.5	More Details
CVE-2023-35940	GLPI is a free asset and IT management software package. Starting in version 9.5.0 and prior to version 10.0.8, an incorrect rights check on a file allows an unauthenticated user to be able to access dashboards data. Version 10.0.8 contains a patch for this issue.	7.5	More Details
CVE-2023-37241	Input verification vulnerability in the WMS API. Successful exploitation of this vulnerability may cause the device to restart.	7.5	More Details
CVE-2023-37239	Format string vulnerability in the distributed file system. Attackers who bypass the selinux permission can exploit this vulnerability to crash the program.	7.5	More Details
CVE-2023-34164	Vulnerability of incomplete input parameter verification in the communication framework module. Successful exploitation of this vulnerability may affect availability.	7.5	More Details
CVE-2023-35920	A vulnerability has been identified in SIMATIC MV540 H (All versions < V3.3.4), SIMATIC MV540 S (All versions < V3.3.4), SIMATIC MV550 H (All versions < V3.3.4), SIMATIC MV550 S (All versions < V3.3.4), SIMATIC MV560 U (All versions < V3.3.4), SIMATIC MV560 X (All versions < V3.3.4). Affected devices cannot properly process specially crafted IP packets sent to the devices. This could allow an unauthenticated remote attacker to cause a denial of service condition. The affected devices must be restarted manually.	7.5	More Details
CVE-2023-1695	Vulnerability of failures to capture exceptions in the communication framework. Successful exploitation of this vulnerability may cause features to perform abnormally.	7.5	More Details
CVE-2023-1691	Vulnerability of failures to capture exceptions in the communication framework. Successful exploitation of this vulnerability may cause features to perform abnormally.	7.5	More Details

CVE Number	Description	Base Score	Reference
CVE-2022-48514	The Sepolicy module has inappropriate permission control on the use of Netlink.Successful exploitation of this vulnerability may affect confidentiality.	7.5	More Details
CVE-2022-48520	Unauthorized access vulnerability in the SystemUI module. Successful exploitation of this vulnerability may affect confidentiality.	7.5	More Details
CVE-2022-48515	Vulnerability of inappropriate permission control in Nearby. Successful exploitation of this vulnerability may affect service confidentiality.	7.5	More Details
CVE-2022-48519	Unauthorized access vulnerability in the SystemUI module. Successful exploitation of this vulnerability may affect confidentiality.	7.5	More Details
CVE-2022-48516	Vulnerability that a unique value can be obtained by a third-party app in the DSoftBus module. Successful exploitation of this vulnerability will affect confidentiality.	7.5	More Details
CVE-2022-23447	An improper limitation of a pathname to a restricted directory ('Path Traversal') vulnerability [CWE-22] in FortiExtender management interface 7.0.0 through 7.0.3, 4.2.0 through 4.2.4, 4.1.1 through 4.1.8, 4.0.0 through 4.0.2, 3.3.0 through 3.3.2, 3.2.1 through 3.2.3, 5.3 all versions may allow an unauthenticated and remote attacker to retrieve arbitrary files from the underlying filesystem via specially crafted web requests.	7.5	More Details
CVE-2023-35309	Microsoft Message Queuing (MSMQ) Remote Code Execution Vulnerability	7.5	More Details
CVE-2022-48507	Vulnerability of identity verification being bypassed in the storage module. Successful exploitation of this vulnerability may affect service confidentiality.	7.5	More Details
CVE-2023-23907	A directory traversal vulnerability exists in the server.js start functionality of Milesight VPN v2.0.2. A specially-crafted network request can lead to arbitrary file read. An attacker can send a network request to trigger this vulnerability.	7.5	More Details

CVE Number	Description	Base Score	Reference
CVE-2023-35921	A vulnerability has been identified in SIMATIC MV540 H (All versions < V3.3.4), SIMATIC MV540 S (All versions < V3.3.4), SIMATIC MV550 H (All versions < V3.3.4), SIMATIC MV550 S (All versions < V3.3.4), SIMATIC MV560 U (All versions < V3.3.4), SIMATIC MV560 X (All versions < V3.3.4). Affected devices cannot properly process specially crafted Ethernet frames sent to the devices. This could allow an unauthenticated remote attacker to cause a denial of service condition. The affected devices must be restarted manually.	7.5	More Details
CVE-2023-33163	Windows Network Load Balancing Remote Code Execution Vulnerability	7.5	More Details
CVE-2023-35298	HTTP.sys Denial of Service Vulnerability	7.5	More Details
CVE-2023-36827	Fides is an open-source privacy engineering platform for managing the fulfillment of data privacy requests in a runtime environment, and the enforcement of privacy regulations in code. A path traversal (directory traversal) vulnerability affects fides versions lower than version `2.15.1`, allowing remote attackers to access arbitrary files on the fides webserver container's filesystem. The vulnerability is patched in fides `2.15.1`. If the Fides webserver API is not directly accessible to attackers and is instead deployed behind a reverse proxy as recommended in Ethyca's security best practice documentation, and the reverse proxy is an AWS application load balancer, the vulnerability can't be exploited by these attackers. An AWS application load balancer will reject this attack with a 400 error. Additionally, any secrets supplied to the container using environment variables rather than a `fides.toml` configuration file are not affected by this vulnerability.	7.5	More Details
CVE-2023-36884	Windows Search Remote Code Execution Vulnerability	7.5	More Details
CVE-2023-32084	HTTP.sys Denial of Service Vulnerability	7.5	More Details
CVE-2023-35352	Windows Remote Desktop Security Feature Bypass Vulnerability	7.5	More Details

CVE Number	Description	Base Score	Reference
CVE-2021-46892	Encryption bypass vulnerability in Maintenance mode. Successful exploitation of this vulnerability may affect service confidentiality.	7.5	More Details
CVE-2023-32045	Microsoft Message Queuing (MSMQ) Denial of Service Vulnerability	7.5	More Details
CVE-2023-32044	Microsoft Message Queuing (MSMQ) Denial of Service Vulnerability	7.5	More Details
CVE-2023-31818	An issue found in Marukyu Line v.13.4.1 allows a remote attacker to gain access to sensitive information via the channel access token in the miniapp function.	7.5	More Details
CVE-2021-46893	Vulnerability of unstrict data verification and parameter check. Successful exploitation of this vulnerability may affect integrity.	7.5	More Details
CVE-2023-36293	SQL injection vulnerability in wmanager v.1.0.7 and before allows a remote attacker to obtain sensitive information via a crafted script to the company.php component.	7.5	More Details
CVE-2023-3354	A flaw was found in the QEMU built-in VNC server. When a client connects to the VNC server, QEMU checks whether the current number of connections crosses a certain threshold and if so, cleans up the previous connection. If the previous connection happens to be in the handshake phase and fails, QEMU cleans up the connection again, resulting in a NULL pointer dereference issue. This could allow a remote unauthenticated client to cause a denial of service.	7.5	More Details
CVE-2023-21526	Windows Netlogon Information Disclosure Vulnerability	7.4	More Details
CVE-2023-29131	A vulnerability has been identified in SIMATIC CN 4100 (All versions < V2.5). Affected device consists of an incorrect default value in the SSH configuration. This could allow an attacker to bypass network isolation.	7.4	More Details
CVE-2021-42080	An attacker is able to launch a Reflected XSS attack using a crafted URL.	7.4	More Details

CVE Number	Description	Base Score	Reference
CVE-2023-36824	Redis is an in-memory database that persists on disk. In Redit 7.0 prior to 7.0.12, extracting key names from a command and a list of arguments may, in some cases, trigger a heap overflow and result in reading random heap memory, heap corruption and potentially remote code execution. Several scenarios that may lead to authenticated users executing a specially crafted `COMMAND GETKEYS` or `COMMAND GETKEYSANDFLAGS`and authenticated users who were set with ACL rules that match key names, executing a specially crafted command that refers to a variadic list of key names. The vulnerability is patched in Redis 7.0.12.	7.4	More Details
CVE-2023-36749	A vulnerability has been identified in RUGGEDCOM ROX MX5000 (All versions < V2.16.0), RUGGEDCOM ROX MX5000RE (All versions < V2.16.0), RUGGEDCOM ROX RX1400 (All versions < V2.16.0), RUGGEDCOM ROX RX1500 (All versions < V2.16.0), RUGGEDCOM ROX RX1501 (All versions < V2.16.0), RUGGEDCOM ROX RX1510 (All versions < V2.16.0), RUGGEDCOM ROX RX1511 (All versions < V2.16.0), RUGGEDCOM ROX RX1512 (All versions < V2.16.0), RUGGEDCOM ROX RX1524 (All versions < V2.16.0), RUGGEDCOM ROX RX1536 (All versions < V2.16.0), RUGGEDCOM ROX RX5000 (All versions < V2.16.0). The webserver of the affected devices support insecure TLS 1.0 protocol. An attacker could achieve a man-in-the-middle attack and compromise confidentiality and integrity of data.	7.4	More Details
CVE-2023-2078	The "Buy Me a Coffee – Button and Widget Plugin" plugin for WordPress is vulnerable to unauthorized modification of data due to missing capability checks on the recieve_post, bmc_disconnect, name_post, and widget_post functions in versions up to, and including, 3.7. This makes it possible for authenticated attackers, with minimal permissions such as subscribers, to update the plugins settings. CVE-2023-25030 may be a duplicate of this issue.	7.3	More Details
CVE-2023-3617	A vulnerability was found in SourceCodester Best POS Management System 1.0. It has been classified as critical. This affects an unknown part of the file admin_class.php of the component Login Page. The manipulation of the argument username leads to sql injection. It is possible to initiate the attack remotely. The exploit has been disclosed to the public and may be used. The identifier VDB-233565 was assigned to this vulnerability.	7.3	More Details
CVE-2023-22319	A sql injection vulnerability exists in the requestHandlers.js LoginAuth functionality of Milesight VPN v2.0.2. A specially-crafted network request can lead to authentication bypass. An attacker can send a malicious packet to trigger this vulnerability.	7.3	More Details

CVE Number	Description	Base Score	Reference
CVE-2023-22844	An authentication bypass vulnerability exists in the requestHandlers.js verifyToken functionality of Milesight VPN v2.0.2. A specially-crafted network request can lead to authentication bypass. An attacker can send a network request to trigger this vulnerability.	7.3	More Details
CVE-2023-36537	Improper privilege management in Zoom Rooms for Windows before version 5.14.5 may allow an authenticated user to enable an escalation of privilege via local access.	7.3	More Details
CVE-2023-34118	Improper privilege management in Zoom Rooms for Windows before version 5.14.5 may allow an authenticated user to enable an escalation of privilege via local access.	7.3	More Details
CVE-2023-32054	Volume Shadow Copy Elevation of Privilege Vulnerability	7.3	More Details
CVE-2023-36921	SAP Solution Manager (Diagnostics agent) - version 7.20, allows an attacker to tamper with headers in a client request. This misleads SAP Diagnostics Agent to serve poisoned content to the server. On successful exploitation, the attacker can cause a limited impact on confidentiality and availability of the application.	7.2	More Details
CVE-2023-23777	An improper neutralization of special elements used in an OS command ('OS Command Injection') vulnerability [CWE-78] in FortiWeb version 7.0.1 and below, 6.4 all versions, version 6.3.18 and below may allow a privileged attacker to execute arbitrary bash commands via crafted cli backup parameters.	7.2	More Details
CVE-2023-36925	SAP Solution Manager (Diagnostics agent) - version 7.20, allows an unauthenticated attacker to blindly execute HTTP requests. On successful exploitation, the attacker can cause a limited impact on confidentiality and availability of the application and other applications the Diagnostics Agent can reach.	7.2	More Details
CVE-2023-36992	PHP injection in TravianZ 8.3.4 and 8.3.3 in the config editor in the admin page allows remote attackers to execute PHP code.	7.2	More Details
CVE-2023-3551	Code Injection in GitHub repository nilsteampassnet/teampass prior to 3.0.10.	7.2	More Details
CVE-2023-35350	Windows Active Directory Certificate Services (AD CS) Remote Code Execution Vulnerability	7.2	More Details

CVE Number	Description	Base Score	Reference
CVE-2023-1208	This HTTP Headers WordPress plugin before 1.18.11 allows arbitrary data to be written to arbitrary files, leading to a Remote Code Execution vulnerability.	7.2	More Details
CVE-2023-2493	The All In One Redirection WordPress plugin before 2.2.0 does not properly sanitise and escape multiple parameters before using them in an SQL statement, leading to a SQL injection exploitable by high privilege users such as admin.	7.2	More Details
CVE-2023-25103	Multiple buffer overflow vulnerabilities exist in the vtysh_ubus binary of Milesight UR32L v32.3.0.5 due to the use of an unsafe sprintf pattern. A specially crafted HTTP request can lead to arbitrary code execution. An attacker with high privileges can send HTTP requests to trigger these vulnerabilities.This buffer overflow occurs in the set_dmvpn function with the gre_ip and the gre_mask variables.	7.2	More Details
CVE-2023-25083	Multiple buffer overflow vulnerabilities exist in the vtysh_ubus binary of Milesight UR32L v32.3.0.5 due to the use of an unsafe sprintf pattern. A specially crafted HTTP request can lead to arbitrary code execution. An attacker with high privileges can send HTTP requests to trigger these vulnerabilities.This buffer overflow occurs in the firewall_handler_set function with the ip and mac variables.	7.2	More Details
CVE-2023-36622	The websocket configuration endpoint of the Loxone Miniserver Go Gen.2 before 14.1.5.9 allows remote authenticated administrators to inject arbitrary OS commands via the timezone parameter.	7.2	More Details
CVE-2023-26137	All versions of the package drogonframework/drogon are vulnerable to HTTP Response Splitting when untrusted user input is used to build header values in the addHeader and addCookie functions. An attacker can add the \r\n (carriage return line feeds) characters to end the HTTP response headers and inject malicious content.	7.2	More Details
CVE-2023-25583	Two OS command injection vulnerabilities exist in the zebra vlan_name functionality of Milesight UR32L v32.3.0.5. A specially crafted network request can lead to command execution. An attacker can send a network request to trigger these vulnerabilities.This command injection is in the code branch that manages a new vlan configuration.	7.2	More Details
CVE-2023-24595	An OS command injection vulnerability exists in the ys_thirdparty system_user_script functionality of Milesight UR32L v32.3.0.5. A specially crafted series of network requests can lead to command execution. An attacker can send a sequence of requests to trigger this vulnerability.	7.2	More Details

CVE Number	Description	Base Score	Reference
CVE-2023-25081	Multiple buffer overflow vulnerabilities exist in the vtysh_ubus binary of Milesight UR32L v32.3.0.5 due to the use of an unsafe sprintf pattern. A specially crafted HTTP request can lead to arbitrary code execution. An attacker with high privileges can send HTTP requests to trigger these vulnerabilities.This buffer overflow occurs in the firewall_handler_set function with the src and dmz variables.	7.2	More Details
CVE-2023-25082	Multiple buffer overflow vulnerabilities exist in the vtysh_ubus binary of Milesight UR32L v32.3.0.5 due to the use of an unsafe sprintf pattern. A specially crafted HTTP request can lead to arbitrary code execution. An attacker with high privileges can send HTTP requests to trigger these vulnerabilities.This buffer overflow occurs in the firewall_handler_set function with the old_ip and old_mac variables.	7.2	More Details
CVE-2023-25107	Multiple buffer overflow vulnerabilities exist in the vtysh_ubus binary of Milesight UR32L v32.3.0.5 due to the use of an unsafe sprintf pattern. A specially crafted HTTP request can lead to arbitrary code execution. An attacker with high privileges can send HTTP requests to trigger these vulnerabilities.This buffer overflow occurs in the set_gre function with the remote_subnet and the remote_mask variables.	7.2	More Details
CVE-2023-25115	Multiple buffer overflow vulnerabilities exist in the vtysh_ubus binary of Milesight UR32L v32.3.0.5 due to the use of an unsafe sprintf pattern. A specially crafted HTTP request can lead to arbitrary code execution. An attacker with high privileges can send HTTP requests to trigger these vulnerabilities.This buffer overflow occurs in the set_openvpn_client function with the remote_ip and the port variables.	7.2	More Details
CVE-2023-25112	Multiple buffer overflow vulnerabilities exist in the vtysh_ubus binary of Milesight UR32L v32.3.0.5 due to the use of an unsafe sprintf pattern. A specially crafted HTTP request can lead to arbitrary code execution. An attacker with high privileges can send HTTP requests to trigger these vulnerabilities.This buffer overflow occurs in the set_l2tp function with the remote_subnet and the remote_mask variables.	7.2	More Details
CVE-2023-25084	Multiple buffer overflow vulnerabilities exist in the vtysh_ubus binary of Milesight UR32L v32.3.0.5 due to the use of an unsafe sprintf pattern. A specially crafted HTTP request can lead to arbitrary code execution. An attacker with high privileges can send HTTP requests to trigger these vulnerabilities.This buffer overflow occurs in the firewall_handler_set function with the ip, mac and description variables.	7.2	More Details

CVE Number	Description	Base Score	Reference
CVE-2023-25114	Multiple buffer overflow vulnerabilities exist in the vtysh_ubus binary of Milesight UR32L v32.3.0.5 due to the use of an unsafe sprintf pattern. A specially crafted HTTP request can lead to arbitrary code execution. An attacker with high privileges can send HTTP requests to trigger these vulnerabilities.This buffer overflow occurs in the set_openvpn_client function with the expert_options variable.	7.2	More Details
CVE-2023-25085	Multiple buffer overflow vulnerabilities exist in the vtysh_ubus binary of Milesight UR32L v32.3.0.5 due to the use of an unsafe sprintf pattern. A specially crafted HTTP request can lead to arbitrary code execution. An attacker with high privileges can send HTTP requests to trigger these vulnerabilities.This buffer overflow occurs in the firewall_handler_set function with the index and to_dst variables.	7.2	More Details
CVE-2023-35973	Authenticated command injection vulnerabilities exist in the ArubaOS command line interface. Successful exploitation of these vulnerabilities result in the ability to execute arbitrary commands as a privileged user on the underlying operating system.	7.2	More Details
CVE-2023-25099	Multiple buffer overflow vulnerabilities exist in the vtysh_ubus binary of Milesight UR32L v32.3.0.5 due to the use of an unsafe sprintf pattern. A specially crafted HTTP request can lead to arbitrary code execution. An attacker with high privileges can send HTTP requests to trigger these vulnerabilities.This buffer overflow occurs in the set_qos function with the dest variable.	7.2	More Details
CVE-2023-25086	Multiple buffer overflow vulnerabilities exist in the vtysh_ubus binary of Milesight UR32L v32.3.0.5 due to the use of an unsafe sprintf pattern. A specially crafted HTTP request can lead to arbitrary code execution. An attacker with high privileges can send HTTP requests to trigger these vulnerabilities.This buffer overflow occurs in the firewall_handler_set function with the index and dport variables.	7.2	More Details
CVE-2023-25113	Multiple buffer overflow vulnerabilities exist in the vtysh_ubus binary of Milesight UR32L v32.3.0.5 due to the use of an unsafe sprintf pattern. A specially crafted HTTP request can lead to arbitrary code execution. An attacker with high privileges can send HTTP requests to trigger these vulnerabilities.This buffer overflow occurs in the set_l2tp function with the key variable.	7.2	More Details
CVE-2023-25582	Two OS command injection vulnerabilities exist in the zebra vlan_name functionality of Milesight UR32L v32.3.0.5. A specially crafted network request can lead to command execution. An attacker can send a network request to trigger these vulnerabilities.This command injection is in the code branch that manages an already existing vlan configuration.	7.2	More Details

CVE Number	Description	Base Score	Reference
CVE-2023-25124	Multiple buffer overflow vulnerabilities exist in the vtysh_ubus binary of Milesight UR32L v32.3.0.5 due to the use of an unsafe sprintf pattern. A specially crafted HTTP request can lead to arbitrary code execution. An attacker with high privileges can send HTTP requests to trigger these vulnerabilities.This buffer overflow occurs in the set_openvpn_client function with the remote_subnet and the remote_mask variables.	7.2	More Details
CVE-2023-25123	Multiple buffer overflow vulnerabilities exist in the vtysh_ubus binary of Milesight UR32L v32.3.0.5 due to the use of an unsafe sprintf pattern. A specially crafted HTTP request can lead to arbitrary code execution. An attacker with high privileges can send HTTP requests to trigger these vulnerabilities.This buffer overflow occurs in the set_openvpn_client function with the remote_subnet and the remote_mask variables when action is 2.	7.2	More Details
CVE-2023-23550	An OS command injection vulnerability exists in the ys_thirdparty user_delete functionality of Milesight UR32L v32.3.0.5. A specially crafted network packet can lead to command execution. An attacker can send a sequence of requests to trigger this vulnerability.	7.2	More Details
CVE-2023-22659	An os command injection vulnerability exists in the libzebra.so change_hostname functionality of Milesight UR32L v32.3.0.5. A specially-crafted network packets can lead to command execution. An attacker can send a sequence of requests to trigger this vulnerability.	7.2	More Details
CVE-2023-35972	An authenticated remote command injection vulnerability exists in the ArubaOS web-based management interface. Successful exploitation of this vulnerability results in the ability to execute arbitrary commands as a privileged user on the underlying operating system. This allows an attacker to fully compromise the underlying operating system on the device running ArubaOS.	7.2	More Details
CVE-2023-22365	An OS command injection vulnerability exists in the ys_thirdparty check_system_user functionality of Milesight UR32L v32.3.0.5. A specially crafted set of network packets can lead to command execution. An attacker can send a network request to trigger this vulnerability.	7.2	More Details
CVE-2023-22306	An OS command injection vulnerability exists in the libzebra.so bridge_group functionality of Milesight UR32L v32.3.0.5. A specially crafted network packet can lead to command execution. An attacker can send a sequence of requests to trigger this vulnerability.	7.2	More Details
CVE-2023-35974	Authenticated command injection vulnerabilities exist in the ArubaOS command line interface. Successful exploitation of these vulnerabilities result in the ability to execute arbitrary commands as a privileged user on the underlying operating system.	7.2	More Details

CVE Number	Description	Base Score	Reference
CVE-2023-25097	Multiple buffer overflow vulnerabilities exist in the vtysh_ubus binary of Milesight UR32L v32.3.0.5 due to the use of an unsafe sprintf pattern. A specially crafted HTTP request can lead to arbitrary code execution. An attacker with high privileges can send HTTP requests to trigger these vulnerabilities.This buffer overflow occurs in the set_qos function with the attach_class variable.	7.2	More Details
CVE-2023-25118	Multiple buffer overflow vulnerabilities exist in the vtysh_ubus binary of Milesight UR32L v32.3.0.5 due to the use of an unsafe sprintf pattern. A specially crafted HTTP request can lead to arbitrary code execution. An attacker with high privileges can send HTTP requests to trigger these vulnerabilities.This buffer overflow occurs in the set_openvpn_client function with the username and the password variables.	7.2	More Details
CVE-2023-25119	Multiple buffer overflow vulnerabilities exist in the vtysh_ubus binary of Milesight UR32L v32.3.0.5 due to the use of an unsafe sprintf pattern. A specially crafted HTTP request can lead to arbitrary code execution. An attacker with high privileges can send HTTP requests to trigger these vulnerabilities.This buffer overflow occurs in the set_pptp function with the remote_subnet and the remote_mask variables.	7.2	More Details
CVE-2023-25116	Multiple buffer overflow vulnerabilities exist in the vtysh_ubus binary of Milesight UR32L v32.3.0.5 due to the use of an unsafe sprintf pattern. A specially crafted HTTP request can lead to arbitrary code execution. An attacker with high privileges can send HTTP requests to trigger these vulnerabilities.This buffer overflow occurs in the set_openvpn_client function with the local_virtual_ip and the remote_virtual_ip variables.	7.2	More Details
CVE-2023-36968	A SQL Injection vulnerability detected in Food Ordering System v1.0 allows attackers to run commands on the database by sending crafted SQL queries to the ID parameter.	7.2	More Details
CVE-2023-25096	Multiple buffer overflow vulnerabilities exist in the vtysh_ubus binary of Milesight UR32L v32.3.0.5 due to the use of an unsafe sprintf pattern. A specially crafted HTTP request can lead to arbitrary code execution. An attacker with high privileges can send HTTP requests to trigger these vulnerabilities.This buffer overflow occurs in the set_qos function with the rule_name variable with two possible format strings.	7.2	More Details
CVE-2023-25120	Multiple buffer overflow vulnerabilities exist in the vtysh_ubus binary of Milesight UR32L v32.3.0.5 due to the use of an unsafe sprintf pattern. A specially crafted HTTP request can lead to arbitrary code execution. An attacker with high privileges can send HTTP requests to trigger these vulnerabilities.This buffer overflow occurs in the set_dmvpn function with the cisco_secret variable.	7.2	More Details

CVE Number	Description	Base Score	Reference
CVE-2023-25121	Multiple buffer overflow vulnerabilities exist in the vtysh_ubus binary of Milesight UR32L v32.3.0.5 due to the use of an unsafe sprintf pattern. A specially crafted HTTP request can lead to arbitrary code execution. An attacker with high privileges can send HTTP requests to trigger these vulnerabilities.This buffer overflow occurs in the set_ike_profile function with the secrets_local variable.	7.2	More Details
CVE-2023-25122	Multiple buffer overflow vulnerabilities exist in the vtysh_ubus binary of Milesight UR32L v32.3.0.5 due to the use of an unsafe sprintf pattern. A specially crafted HTTP request can lead to arbitrary code execution. An attacker with high privileges can send HTTP requests to trigger these vulnerabilities.This buffer overflow occurs in the set_openvpn_client function with the old_remote_subnet and the old_remote_mask variables.	7.2	More Details
CVE-2023-25098	Multiple buffer overflow vulnerabilities exist in the vtysh_ubus binary of Milesight UR32L v32.3.0.5 due to the use of an unsafe sprintf pattern. A specially crafted HTTP request can lead to arbitrary code execution. An attacker with high privileges can send HTTP requests to trigger these vulnerabilities.This buffer overflow occurs in the set_qos function with the source variable.	7.2	More Details
CVE-2023-25100	Multiple buffer overflow vulnerabilities exist in the vtysh_ubus binary of Milesight UR32L v32.3.0.5 due to the use of an unsafe sprintf pattern. A specially crafted HTTP request can lead to arbitrary code execution. An attacker with high privileges can send HTTP requests to trigger these vulnerabilities.This buffer overflow occurs in the set_qos function with the default_class variable.	7.2	More Details
CVE-2023-25117	Multiple buffer overflow vulnerabilities exist in the vtysh_ubus binary of Milesight UR32L v32.3.0.5 due to the use of an unsafe sprintf pattern. A specially crafted HTTP request can lead to arbitrary code execution. An attacker with high privileges can send HTTP requests to trigger these vulnerabilities.This buffer overflow occurs in the set_openvpn_client function with the local_virtual_ip and the local_virtual_mask variables.	7.2	More Details
CVE-2023-25092	Multiple buffer overflow vulnerabilities exist in the vtysh_ubus binary of Milesight UR32L v32.3.0.5 due to the use of an unsafe sprintf pattern. A specially crafted HTTP request can lead to arbitrary code execution. An attacker with high privileges can send HTTP requests to trigger these vulnerabilities.This buffer overflow occurs in the handle_interface_acl function with the interface and out_acl variables.	7.2	More Details

CVE Number	Description	Base Score	Reference
CVE-2023-25108	Multiple buffer overflow vulnerabilities exist in the vtysh_ubus binary of Milesight UR32L v32.3.0.5 due to the use of an unsafe sprintf pattern. A specially crafted HTTP request can lead to arbitrary code execution. An attacker with high privileges can send HTTP requests to trigger these vulnerabilities.This buffer overflow occurs in the set_gre function with the remote_ip variable.	7.2	More Details
CVE-2023-25095	Multiple buffer overflow vulnerabilities exist in the vtysh_ubus binary of Milesight UR32L v32.3.0.5 due to the use of an unsafe sprintf pattern. A specially crafted HTTP request can lead to arbitrary code execution. An attacker with high privileges can send HTTP requests to trigger these vulnerabilities.This buffer overflow occurs in the set_qos function with the rule_name variable with two possible format strings that represent negated commands.	7.2	More Details
CVE-2023-25094	Multiple buffer overflow vulnerabilities exist in the vtysh_ubus binary of Milesight UR32L v32.3.0.5 due to the use of an unsafe sprintf pattern. A specially crafted HTTP request can lead to arbitrary code execution. An attacker with high privileges can send HTTP requests to trigger these vulnerabilities.This buffer overflow occurs in the into_class_node function with either the class_name or old_class_name variable.	7.2	More Details
CVE-2023-25109	Multiple buffer overflow vulnerabilities exist in the vtysh_ubus binary of Milesight UR32L v32.3.0.5 due to the use of an unsafe sprintf pattern. A specially crafted HTTP request can lead to arbitrary code execution. An attacker with high privileges can send HTTP requests to trigger these vulnerabilities.This buffer overflow occurs in the set_gre function with the local_ip variable.	7.2	More Details
CVE-2023-25105	Multiple buffer overflow vulnerabilities exist in the vtysh_ubus binary of Milesight UR32L v32.3.0.5 due to the use of an unsafe sprintf pattern. A specially crafted HTTP request can lead to arbitrary code execution. An attacker with high privileges can send HTTP requests to trigger these vulnerabilities.This buffer overflow occurs in the set_ike_profile function with the secrets_remote variable.	7.2	More Details
CVE-2023-25110	Multiple buffer overflow vulnerabilities exist in the vtysh_ubus binary of Milesight UR32L v32.3.0.5 due to the use of an unsafe sprintf pattern. A specially crafted HTTP request can lead to arbitrary code execution. An attacker with high privileges can send HTTP requests to trigger these vulnerabilities.This buffer overflow occurs in the set_gre function with the remote_virtual_ip variable.	7.2	More Details

CVE Number	Description	Base Score	Reference
CVE-2023-25093	Multiple buffer overflow vulnerabilities exist in the vtysh_ubus binary of Milesight UR32L v32.3.0.5 due to the use of an unsafe sprintf pattern. A specially crafted HTTP request can lead to arbitrary code execution. An attacker with high privileges can send HTTP requests to trigger these vulnerabilities.This buffer overflow occurs in the set_qos function with the class_name variable..	7.2	More Details
CVE-2023-25104	Multiple buffer overflow vulnerabilities exist in the vtysh_ubus binary of Milesight UR32L v32.3.0.5 due to the use of an unsafe sprintf pattern. A specially crafted HTTP request can lead to arbitrary code execution. An attacker with high privileges can send HTTP requests to trigger these vulnerabilities.This buffer overflow occurs in the set_ike_profile function with the username and the password variables.	7.2	More Details
CVE-2023-25106	Multiple buffer overflow vulnerabilities exist in the vtysh_ubus binary of Milesight UR32L v32.3.0.5 due to the use of an unsafe sprintf pattern. A specially crafted HTTP request can lead to arbitrary code execution. An attacker with high privileges can send HTTP requests to trigger these vulnerabilities.This buffer overflow occurs in the set_gre function with the local_virtual_ip and the local_virtual_mask variables.	7.2	More Details
CVE-2023-25101	Multiple buffer overflow vulnerabilities exist in the vtysh_ubus binary of Milesight UR32L v32.3.0.5 due to the use of an unsafe sprintf pattern. A specially crafted HTTP request can lead to arbitrary code execution. An attacker with high privileges can send HTTP requests to trigger these vulnerabilities.This buffer overflow occurs in the set_dmvpn function with the gre_key variable.	7.2	More Details
CVE-2023-25091	Multiple buffer overflow vulnerabilities exist in the vtysh_ubus binary of Milesight UR32L v32.3.0.5 due to the use of an unsafe sprintf pattern. A specially crafted HTTP request can lead to arbitrary code execution. An attacker with high privileges can send HTTP requests to trigger these vulnerabilities.This buffer overflow occurs in the handle_interface_acl function with the interface variable when out_acl is -1.	7.2	More Details
CVE-2023-25090	Multiple buffer overflow vulnerabilities exist in the vtysh_ubus binary of Milesight UR32L v32.3.0.5 due to the use of an unsafe sprintf pattern. A specially crafted HTTP request can lead to arbitrary code execution. An attacker with high privileges can send HTTP requests to trigger these vulnerabilities.This buffer overflow occurs in the handle_interface_acl function with the interface and in_acl variables.	7.2	More Details

CVE Number	Description	Base Score	Reference
CVE-2023-25089	Multiple buffer overflow vulnerabilities exist in the vtysh_ubus binary of Milesight UR32L v32.3.0.5 due to the use of an unsafe sprintf pattern. A specially crafted HTTP request can lead to arbitrary code execution. An attacker with high privileges can send HTTP requests to trigger these vulnerabilities.This buffer overflow occurs in the handle_interface_acl function with the interface variable when in_acl is -1.	7.2	More Details
CVE-2023-25088	Multiple buffer overflow vulnerabilities exist in the vtysh_ubus binary of Milesight UR32L v32.3.0.5 due to the use of an unsafe sprintf pattern. A specially crafted HTTP request can lead to arbitrary code execution. An attacker with high privileges can send HTTP requests to trigger these vulnerabilities.This buffer overflow occurs in the firewall_handler_set function with the index and description variables.	7.2	More Details
CVE-2023-25111	Multiple buffer overflow vulnerabilities exist in the vtysh_ubus binary of Milesight UR32L v32.3.0.5 due to the use of an unsafe sprintf pattern. A specially crafted HTTP request can lead to arbitrary code execution. An attacker with high privileges can send HTTP requests to trigger these vulnerabilities.This buffer overflow occurs in the set_gre function with the key variable.	7.2	More Details
CVE-2023-25102	Multiple buffer overflow vulnerabilities exist in the vtysh_ubus binary of Milesight UR32L v32.3.0.5 due to the use of an unsafe sprintf pattern. A specially crafted HTTP request can lead to arbitrary code execution. An attacker with high privileges can send HTTP requests to trigger these vulnerabilities.This buffer overflow occurs in the set_dmvpn function with the hub_ip and the hub_gre_ip variables.	7.2	More Details
CVE-2023-25087	Multiple buffer overflow vulnerabilities exist in the vtysh_ubus binary of Milesight UR32L v32.3.0.5 due to the use of an unsafe sprintf pattern. A specially crafted HTTP request can lead to arbitrary code execution. An attacker with high privileges can send HTTP requests to trigger these vulnerabilities.This buffer overflow occurs in the firewall_handler_set function with the index and to_dport variables.	7.2	More Details

CVE Number	Description	Base Score	Reference
CVE-2023-36823	Sanitize is an allowlist-based HTML and CSS sanitizer. Using carefully crafted input, an attacker may be able to sneak arbitrary HTML and CSS through Sanitize starting with version 3.0.0 and prior to version 6.0.2 when Sanitize is configured to use the built-in "relaxed" config or when using a custom config that allows `style` elements and one or more CSS at-rules. This could result in cross-site scripting or other undesired behavior when the malicious HTML and CSS are rendered in a browser. Sanitize 6.0.2 performs additional escaping of CSS in `style` element content, which fixes this issue. Users who are unable to upgrade can prevent this issue by using a Sanitize config that doesn't allow `style` elements, using a Sanitize config that doesn't allow CSS at-rules, or by manually escaping the character sequence `</` as `<\/` in `style` element content.	7.1	More Details
CVE-2023-34338	AMI SPx contains a vulnerability in the BMC where an Attacker may cause a use of hard-coded cryptographic key by a hard-coded certificate. A successful exploit of this vulnerability may lead to a loss of confidentiality, integrity, and availability.	7.1	More Details
CVE-2023-35347	Microsoft Install Service Elevation of Privilege Vulnerability	7.1	More Details
CVE-2023-36813	Kanboard is project management software that focuses on the Kanban methodology. In versions prior to 1.2.31authenticated user is able to perform a SQL Injection, leading to a privilege escalation or loss of confidentiality. It appears that in some insert and update operations, the code improperly uses the PicoDB library to update/insert new information. Version 1.2.31 contains a fix for this issue.	7.1	More Details
CVE-2023-3523	Out-of-bounds Read in GitHub repository gpac/gpac prior to 2.2.2.	7.1	More Details
CVE-2023-23671	Cross-Site Request Forgery (CSRF) vulnerability in Muneeb Layer Slider plugin <= 1.1.9.7 versions.	7.1	More Details
CVE-2023-32050	Windows Installer Elevation of Privilege Vulnerability	7.0	More Details
CVE-2023-35360	Windows Kernel Elevation of Privilege Vulnerability	7.0	More Details

CVE Number	Description	Base Score	Reference
CVE-2023-35361	Windows Kernel Elevation of Privilege Vulnerability	7.0	More Details
CVE-2023-33152	Microsoft ActiveX Remote Code Execution Vulnerability	7.0	More Details
CVE-2023-28958	IBM Watson Knowledge Catalog on Cloud Pak for Data 4.0 is potentially vulnerable to CSV Injection. A remote attacker could execute arbitrary commands on the system, caused by improper validation of csv file contents. IBM X-Force ID: 251782.	7.0	More Details
CVE-2023-3089	A compliance problem was found in the Red Hat OpenShift Container Platform. Red Hat discovered that, when FIPS mode was enabled, not all of the cryptographic modules in use were FIPS-validated.	7.0	More Details
CVE-2023-36829	Sentry is an error tracking and performance monitoring platform. Starting in version 23.6.0 and prior to version 23.6.2, the Sentry API incorrectly returns the `access-control-allow-credentials: true` HTTP header if the `Origin` request header ends with the `system.base-hostname` option of Sentry installation. This only affects installations that have `system.base-hostname` option explicitly set, as it is empty by default. Impact is limited since recent versions of major browsers have cross-site cookie blocking enabled by default. However, this flaw could allow other multi-step attacks. The patch has been released in Sentry 23.6.2.	6.8	More Details
CVE-2023-27198	PAX A930 device with PayDroid_7.1.1_Virgo_V04.5.02_20220722 can allow the execution of arbitrary commands by using the exec service and including a specific word in the command to be executed. The attacker must have physical USB access to the device in order to exploit this vulnerability.	6.8	More Details
CVE-2023-32043	Windows Remote Desktop Security Feature Bypass Vulnerability	6.8	More Details
CVE-2023-33153	Microsoft Outlook Remote Code Execution Vulnerability	6.8	More Details
CVE-2023-35332	Windows Remote Desktop Protocol Security Feature Bypass	6.8	More Details

CVE Number	Description	Base Score	Reference
CVE-2023-2234	Union variant confusion allows any malicious BT controller to execute arbitrary code on the Zephyr host.	6.8	More Details
CVE-2023-30672	Improper privilege management vulnerability in Samsung Smart Switch for Windows Installer prior to version 4.3.23043_3 allows attackers to cause permanent DoS via directory junction.	6.8	More Details
CVE-2023-30652	Out of bounds read and write in callrunTspCmdNoRead of sysinput HAL service prior to SMR Jul-2023 Release 1 allows local attackers to execute arbitrary code.	6.7	More Details
CVE-2023-30670	Out-of-bounds Write in BuildIpcFactoryDeviceTestEvent of libsec-ril prior to SMR Jul-2023 Release 1 allows local attacker to execute arbitrary code.	6.7	More Details
CVE-2023-32055	Active Template Library Elevation of Privilege Vulnerability	6.7	More Details
CVE-2023-30669	Out-of-bounds Write in DoOemFactorySendFactoryTestResult of libsec-ril prior to SMR Jul-2023 Release 1 allows local attacker to execute arbitrary code.	6.7	More Details
CVE-2023-30668	Out-of-bounds Write in BuildOemSecureSimLockResponse of libsec-ril prior to SMR Jul-2023 Release 1 allows local attacker to execute arbitrary code.	6.7	More Details
CVE-2023-27199	PAX Technology A930 PayDroid_7.1.1_Virgo_V04.5.02_20220722 allows attackers to compile a malicious shared library and use LD_PRELOAD to bypass authorization checks.	6.7	More Details
CVE-2023-30651	Out of bounds read and write in callgetTspsysfs of sysinput HAL service prior to SMR Jul-2023 Release 1 allows local attackers to execute arbitrary code.	6.7	More Details
CVE-2023-27197	PAX A930 device with PayDroid_7.1.1_Virgo_V04.5.02_20220722 can allow an attacker to gain root access by running a crafted binary leveraging an exported function from a shared library. The attacker must have shell access to the device in order to exploit this vulnerability.	6.7	More Details
CVE-2023-30653	Out of bounds read and write in enableTspDevice of sysinput HAL service prior to SMR Jul-2023 Release 1 allows local attackers to execute arbitrary code.	6.7	More Details

CVE Number	Description	Base Score	Reference
CVE-2023-30650	Out of bounds read and write in callrunTspCmd of sysinput HAL service prior to SMR Jul-2023 Release 1 allows local attackers to execute arbitrary code.	6.7	More Details
CVE-2023-35351	Windows Active Directory Certificate Services (AD CS) Remote Code Execution Vulnerability	6.6	More Details
CVE-2023-35310	Windows DNS Server Remote Code Execution Vulnerability	6.6	More Details
CVE-2023-35346	Windows DNS Server Remote Code Execution Vulnerability	6.6	More Details
CVE-2023-35345	Windows DNS Server Remote Code Execution Vulnerability	6.6	More Details
CVE-2023-34473	AMI SPx contains a vulnerability in the BMC where a valid user may cause a use of hard-coded credentials. A successful exploit of this vulnerability may lead to a loss of confidentiality, integrity, and availability.	6.6	More Details
CVE-2023-35344	Windows DNS Server Remote Code Execution Vulnerability	6.6	More Details
CVE-2023-32033	Microsoft Failover Cluster Remote Code Execution Vulnerability	6.6	More Details
CVE-2023-36822	Uptime Kuma, a self-hosted monitoring tool, has a path traversal vulnerability in versions prior to 1.22.1. Uptime Kuma allows authenticated users to install plugins from an official list of plugins. This feature is currently disabled in the web interface, but the corresponding API endpoints are still available after login. Before a plugin is downloaded, the plugin installation directory is checked for existence. If it exists, it's removed before the plugin installation. Because the plugin is not validated against the official list of plugins or sanitized, the check for existence and the removal of the plugin installation directory are prone to path traversal. This vulnerability allows an authenticated attacker to delete files from the server Uptime Kuma is running on. Depending on which files are deleted, Uptime Kuma or the whole system may become unavailable due to data loss.	6.5	More Details

CVE Number	Description	Base Score	Reference
CVE-2023-3605	A vulnerability was found in PHPGurukul Online Shopping Portal 1.0. It has been declared as critical. Affected by this vulnerability is an unknown functionality of the component Registration Page. The manipulation leads to improper restriction of excessive authentication attempts. The attack can be launched remotely. The associated identifier of this vulnerability is VDB-233467.	6.5	More Details
CVE-2023-33172	Remote Procedure Call Runtime Denial of Service Vulnerability	6.5	More Details
CVE-2023-37204	A website could have obscured the fullscreen notification by using an option element by introducing lag via an expensive computational function. This could have led to user confusion and possible spoofing attacks. This vulnerability affects Firefox < 115.	6.5	More Details
CVE-2023-35975	An authenticated path traversal vulnerability exists in the ArubaOS command line interface. Successful exploitation of this vulnerability results in the ability to delete arbitrary files in the underlying operating system.	6.5	More Details
CVE-2023-35976	Vulnerabilities exist which allow an authenticated attacker to access sensitive information on the ArubaOS command line interface. Successful exploitation could allow access to data beyond what is authorized by the users existing privilege level.	6.5	More Details
CVE-2023-30674	Improper configuration in Samsung Internet prior to version 21.0.0.41 allows attacker to bypass SameSite Cookie.	6.5	More Details
CVE-2023-29406	The HTTP/1 client does not fully validate the contents of the Host header. A maliciously crafted Host header can inject additional headers or entire requests. With fix, the HTTP/1 client now refuses to send requests containing an invalid Request.Host or Request.URL.Host value.	6.5	More Details
CVE-2023-37207	A website could have obscured the fullscreen notification by using a URL with a scheme handled by an external program, such as a mailto URL. This could have led to user confusion and possible spoofing attacks. This vulnerability affects Firefox < 115, Firefox ESR < 102.13, and Thunderbird < 102.13.	6.5	More Details
CVE-2023-34150	** UNSUPPORTED WHEN ASSIGNED ** Use of TikaEncodingDetector in Apache Any23 can cause excessive memory usage.	6.5	More Details

CVE Number	Description	Base Score	Reference
CVE-2023-35977	Vulnerabilities exist which allow an authenticated attacker to access sensitive information on the ArubaOS command line interface. Successful exploitation could allow access to data beyond what is authorized by the users existing privilege level.	6.5	More Details
CVE-2023-32083	Microsoft Failover Cluster Information Disclosure Vulnerability	6.5	More Details
CVE-2023-34316	An attacker could bypass the latest Delta Electronics InfraSuite Device Master (versions prior to 1.0.7) patch, which could allow an attacker to retrieve file contents.	6.5	More Details
CVE-2023-35316	Remote Procedure Call Runtime Information Disclosure Vulnerability	6.5	More Details
CVE-2023-34107	GLPI is a free asset and IT management software package. Versions of the software starting with 9.2.0 and prior to 10.0.8 have an incorrect rights check on a on a file accessible by an authenticated user, allows access to the view all KnowbaseItems. Version 10.0.8 has a patch for this issue.	6.5	More Details
CVE-2023-34244	GLPI is a free asset and IT management software package. Starting in version 9.4.0 and prior to version 10.0.8, a malicious link can be crafted by an unauthenticated user that can exploit a reflected XSS in case any authenticated user opens the crafted link. Users should upgrade to version 10.0.8 to receive a patch.	6.5	More Details
CVE-2023-33151	Microsoft Outlook Spoofing Vulnerability	6.5	More Details
CVE-2023-35318	Remote Procedure Call Runtime Denial of Service Vulnerability	6.5	More Details
CVE-2023-35765	PiiGAB M-Bus stores credentials in a plaintext file, which could allow a low-level user to gain admin credentials.	6.5	More Details
CVE-2023-35319	Remote Procedure Call Runtime Denial of Service Vulnerability	6.5	More Details
CVE-2023-35348	Active Directory Federation Service Security Feature Bypass Vulnerability	6.5	More Details

CVE Number	Description	Base Score	Reference
CVE-2023-37131	A Cross-Site Request Forgery (CSRF) in the component /public/admin/profile/update.html of YznCMS v1.1.0 allows attackers to arbitrarily change the Administrator password via a crafted POST request.	6.5	More Details
CVE-2023-35321	Windows Deployment Services Denial of Service Vulnerability	6.5	More Details
CVE-2023-33164	Remote Procedure Call Runtime Denial of Service Vulnerability	6.5	More Details
CVE-2023-33166	Remote Procedure Call Runtime Denial of Service Vulnerability	6.5	More Details
CVE-2023-33167	Remote Procedure Call Runtime Denial of Service Vulnerability	6.5	More Details
CVE-2023-33168	Remote Procedure Call Runtime Denial of Service Vulnerability	6.5	More Details
CVE-2023-33169	Remote Procedure Call Runtime Denial of Service Vulnerability	6.5	More Details
CVE-2023-33173	Remote Procedure Call Runtime Denial of Service Vulnerability	6.5	More Details
CVE-2023-23547	A directory traversal vulnerability exists in the luci2-io file-export mib functionality of Milesight UR32L v32.3.0.5. A specially crafted network request can lead to arbitrary file read. An attacker can send a network request to trigger this vulnerability.	6.5	More Details
CVE-2023-32042	OLE Automation Information Disclosure Vulnerability	6.5	More Details
CVE-2023-32037	Windows Layer-2 Bridge Network Driver Information Disclosure Vulnerability	6.5	More Details

CVE Number	Description	Base Score	Reference
CVE-2023-35308	Windows MSHTML Platform Security Feature Bypass Vulnerability	6.5	More Details
CVE-2023-35873	The Runtime Workbench (RWB) of SAP NetWeaver Process Integration - version SAP_XITOOL 7.50, does not perform authentication checks for certain functionalities that require user identity. An unauthenticated user might access technical data about the product status and its configuration. The vulnerability does not allow access to sensitive information or administrative functionalities. On successful exploitation an attacker can cause limited impact on confidentiality and availability of the application.	6.5	More Details
CVE-2023-35336	Windows MSHTML Platform Security Feature Bypass Vulnerability	6.5	More Details
CVE-2023-34106	GLPI is a free asset and IT management software package. Versions of the software starting with 0.68 and prior to 10.0.8 have an incorrect rights check on a on a file accessible by an authenticated user. This allows access to the list of all users and their personal information. Users should upgrade to version 10.0.8 to receive a patch.	6.5	More Details
CVE-2023-35331	Windows Local Security Authority (LSA) Denial of Service Vulnerability	6.5	More Details
CVE-2023-3482	When Firefox is configured to block storage of all cookies, it was still possible to store data in localstorage by using an iframe with a source of 'about:blank'. This could have led to malicious websites storing tracking data without permission. This vulnerability affects Firefox < 115.	6.5	More Details
CVE-2023-28955	IBM Watson Knowledge Catalog on Cloud Pak for Data 4.0 could allow an authenticated user send a specially crafted request that could cause a denial of service. IBM X-Force ID: 251704.	6.5	More Details
CVE-2023-37210	A website could prevent a user from exiting full-screen mode via alert and prompt calls. This could lead to user confusion and possible spoofing attacks. This vulnerability affects Firefox < 115.	6.5	More Details
CVE-2023-3574	Improper Authorization in GitHub repository pimcore/customer-data-framework prior to 3.4.1.	6.5	More Details

CVE Number	Description	Base Score	Reference
CVE-2023-35872	The Message Display Tool (MDT) of SAP NetWeaver Process Integration - version SAP_XIAF 7.50, does not perform authentication checks for certain functionalities that require user identity. An unauthenticated user might access technical data about the product status and its configuration. The vulnerability does not allow access to sensitive information or administrative functionalities. On successful exploitation an attacker can cause limited impact on confidentiality and availability of the application.	6.5	More Details
CVE-2023-25606	An improper limitation of a pathname to a restricted directory ('Path Traversal') vulnerability [CWE-23] in FortiAnalyzer and FortiManager management interface 7.2.0 through 7.2.1, 7.0.0 through 7.0.5, 6.4 all versions may allow a remote and authenticated attacker to retrieve arbitrary files from the underlying filesystem via specially crafted web requests.	6.5	More Details
CVE-2023-35296	Microsoft PostScript and PCL6 Class Printer Driver Information Disclosure Vulnerability	6.5	More Details
CVE-2023-32035	Remote Procedure Call Runtime Denial of Service Vulnerability	6.5	More Details
CVE-2023-35329	Windows Authentication Denial of Service Vulnerability	6.5	More Details
CVE-2023-36868	Azure Service Fabric on Windows Information Disclosure Vulnerability	6.5	More Details
CVE-2023-35314	Remote Procedure Call Runtime Denial of Service Vulnerability	6.5	More Details
CVE-2023-32034	Remote Procedure Call Runtime Denial of Service Vulnerability	6.5	More Details
CVE-2023-20575	A potential power side-channel vulnerability in some AMD processors may allow an authenticated attacker to use the power reporting functionality to monitor a program’s execution inside an AMD SEV VM potentially resulting in a leak of sensitive information.	6.5	More Details

CVE Number	Description	Base Score	Reference
CVE-2023-36256	The Online Examination System Project 1.0 version is vulnerable to Cross-Site Request Forgery (CSRF) attacks. An attacker can craft a malicious link that, when clicked by an admin user, will delete a user account from the database without the admin's consent. The email of the user to be deleted is passed as a parameter in the URL, which can be manipulated by the attacker. This could result in a loss of data.	6.5	More Details
CVE-2023-36871	Azure Active Directory Security Feature Bypass Vulnerability	6.5	More Details
CVE-2023-24881	Microsoft Teams Information Disclosure Vulnerability	6.5	More Details
CVE-2023-37205	The use of RTL Arabic characters in the address bar may have allowed for URL spoofing. This vulnerability affects Firefox < 115.	6.5	More Details
CVE-2023-37206	Uploading files which contain symlinks may have allowed an attacker to trick a user into submitting sensitive data to a malicious website. This vulnerability affects Firefox < 115.	6.5	More Details
CVE-2023-37288	SmartBPM.NET component has a vulnerability of path traversal within its file download function. An unauthenticated remote attacker can exploit this vulnerability to access arbitrary system files.	6.5	More Details
CVE-2021-39014	IBM Cloud Object System 3.15.8.97 is vulnerable to stored 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: 213650.	6.4	More Details
CVE-2023-3606	A vulnerability was found in TamronOS up to 20230703. It has been classified as critical. This affects an unknown part of the file /api/ping. The manipulation of the argument host leads to os command injection. It is possible to initiate the attack remotely. The exploit has been disclosed to the public and may be used. The associated identifier of this vulnerability is VDB-233475. NOTE: The vendor was contacted early about this disclosure but did not respond in any way.	6.3	More Details

CVE Number	Description	Base Score	Reference
CVE-2023-3599	A vulnerability was found in SourceCodester Best Fee Management System 1.0. It has been rated as critical. Affected by this issue is the function save_user of the file admin_class.php of the component Add User Handler. The manipulation leads to improper access controls. The attack may be launched remotely. The exploit has been disclosed to the public and may be used. VDB-233450 is the identifier assigned to this vulnerability.	6.3	More Details
CVE-2023-35870	When creating a journal entry template in SAP S/4HANA (Manage Journal Entry Template) - versions S4CORE 104, 105, 106, 107, an attacker could intercept the save request and change the template, leading to an impact on confidentiality and integrity of the resource. Furthermore, a standard template could be deleted, hence making the resource temporarily unavailable.	6.3	More Details
CVE-2023-34471	AMI SPx contains a vulnerability in the BMC where a user may cause a missing cryptographic step by generating a hash-based message authentication code (HMAC). A successful exploit of this vulnerability may lead to the loss confidentiality, integrity, and authentication.	6.3	More Details
CVE-2023-24487	Arbitrary file read in Citrix ADC and Citrix Gateway	6.3	More Details
CVE-2023-24490	Users with only access to launch VDA applications can launch an unauthorized desktop	6.3	More Details
CVE-2023-3568	Open Redirect in GitHub repository alextselegidis/easyappointments prior to 1.5.0.	6.3	More Details
CVE-2023-27869	IBM Db2 JDBC Driver for Db2 for Linux, UNIX and Windows 10.5, 11.1, and 11.5 could allow a remote authenticated attacker to execute arbitrary code on the system, caused by an unchecked logger injection. By sending a specially crafted request using the named traceFile property, an attacker could exploit this vulnerability to execute arbitrary code on the system. IBM X-Force ID: 249517.	6.3	More Details
CVE-2023-3621	A vulnerability was found in IBOS OA 4.5.5. It has been classified as critical. Affected is the function createDeleteCommand of the file ?r=article/default/delete of the component Delete Packet. The manipulation leads to sql injection. It is possible to launch the attack remotely. The exploit has been disclosed to the public and may be used. VDB-233574 is the identifier assigned to this vulnerability. NOTE: The vendor was contacted early about this disclosure but did not respond in any way.	6.3	More Details

CVE Number	Description	Base Score	Reference
CVE-2023-3619	A vulnerability was found in SourceCodester AC Repair and Services System 1.0 and classified as critical. This issue affects some unknown processing of the file Master.php?f=save_service of the component HTTP POST Request Handler. The manipulation of the argument id leads to sql injection. The attack may be initiated remotely. The identifier VDB-233573 was assigned to this vulnerability.	6.3	More Details
CVE-2023-3534	A vulnerability was found in SourceCodester Shopping Website 1.0. It has been classified as critical. Affected is an unknown function of the file check_availability.php. The manipulation of the argument email leads to sql injection. It is possible to launch the attack remotely. The exploit has been disclosed to the public and may be used. VDB-233286 is the identifier assigned to this vulnerability.	6.3	More Details
CVE-2023-3626	A vulnerability, which was classified as critical, has been found in Suncreate Mountain Flood Disaster Prevention Monitoring and Early Warning System up to 20230706. This issue affects some unknown processing of the file /Duty/AjaxHandle/UpLoadFloodPlanFile.ashx of the component UpLoadFloodPlanFile. The manipulation of the argument Filedata leads to unrestricted upload. The attack may be initiated remotely. The exploit has been disclosed to the public and may be used. The associated identifier of this vulnerability is VDB-233579. NOTE: The vendor was contacted early about this disclosure but did not respond in any way.	6.3	More Details
CVE-2023-3625	A vulnerability classified as critical was found in Suncreate Mountain Flood Disaster Prevention Monitoring and Early Warning System up to 20230706. This vulnerability affects unknown code of the file /Duty/AjaxHandle/Write/UploadFile.ashx of the component Duty Write-UploadFile. The manipulation of the argument Filedata leads to unrestricted upload. The attack can be initiated remotely. The exploit has been disclosed to the public and may be used. VDB-233578 is the identifier assigned to this vulnerability. NOTE: The vendor was contacted early about this disclosure but did not respond in any way.	6.3	More Details
CVE-2023-3624	A vulnerability classified as critical has been found in Nesote Inout Blockchain FiatExchanger 3.0. This affects an unknown part of the file /index.php/coins/update_marketboxslider of the component POST Parameter Handler. The manipulation of the argument marketcurrency leads to sql injection. It is possible to initiate the attack remotely. The identifier VDB-233577 was assigned to this vulnerability. NOTE: The vendor was contacted early about this disclosure but did not respond in any way.	6.3	More Details

CVE Number	Description	Base Score	Reference
CVE-2023-3623	A vulnerability was found in Suncreate Mountain Flood Disaster Prevention Monitoring and Early Warning System up to 20230704. It has been rated as critical. Affected by this issue is some unknown functionality of the file /Duty/AjaxHandle/UploadHandler.ashx of the component Duty Module. The manipulation of the argument Filedata leads to unrestricted upload. The attack may be launched remotely. The exploit has been disclosed to the public and may be used. The identifier of this vulnerability is VDB-233576. NOTE: The vendor was contacted early about this disclosure but did not respond in any way.	6.3	More Details
CVE-2023-33156	Microsoft Defender Elevation of Privilege Vulnerability	6.3	More Details
CVE-2023-30671	Logic error in package installation via adb command prior to SMR Jul-2023 Release 1 allows local attackers to downgrade installed application.	6.3	More Details
CVE-2023-36830	SQLFluff is a SQL linter. Prior to version 2.1.2, in environments where untrusted users have access to the config files, there is a potential security vulnerability where those users could use the `library_path` config value to allow arbitrary python code to be executed via macros. For many users who use SQLFluff in the context of an environment where all users already have fairly escalated privileges, this may not be an issue - however in larger user bases, or where SQLFluff is bundled into another tool where developers still wish to give users access to supply their on rule configuration, this may be an issue. The 2.1.2 release offers the ability for the `library_path` argument to be overwritten on the command line by using the `--library-path` option. This overrides any values provided in the config files and effectively prevents this route of attack for users which have access to the config file, but not to the scripts which call the SQLFluff CLI directly. A similar option is provided for the Python API, where users also have a greater ability to further customise or override configuration as necessary. Unless `library_path` is explicitly required, SQLFluff maintainers recommend using the option `--library-path none` when invoking SQLFluff which will disable the `library-path` option entirely regardless of the options set in the configuration file or via inline config directives. As a workaround, limiting access to - or otherwise validating configuration files before they are ingested by SQLFluff will provides a similar effect and does not require upgrade.	6.3	More Details

CVE Number	Description	Base Score	Reference
CVE-2023-27867	IBM Db2 JDBC Driver for Db2 for Linux, UNIX and Windows 10.5, 11.1, and 11.5 could allow a remote authenticated attacker to execute arbitrary code via JNDI Injection. By sending a specially crafted request using the property clientRerouteServerListJNDIName, an attacker could exploit this vulnerability to execute arbitrary code on the system. IBM X-Force ID: 249514.	6.3	More Details
CVE-2023-27868	IBM Db2 JDBC Driver for Db2 for Linux, UNIX and Windows 10.5, 11.1, and 11.5 could allow a remote authenticated attacker to execute arbitrary code on the system, caused by an unchecked class instantiation when providing plugin classes. By sending a specially crafted request using the named pluginClassName class, an attacker could exploit this vulnerability to execute arbitrary code on the system. IBM X-Force ID: 249516.	6.3	More Details
CVE-2023-36458	1Panel is an open source Linux server operation and maintenance management panel. Prior to version 1.3.6, an authenticated attacker can craft a malicious payloads to achieve command injection when entering the container terminal. The vulnerability has been fixed in v1.3.6.	6.3	More Details
CVE-2023-36457	1Panel is an open source Linux server operation and maintenance management panel. Prior to version 1.3.6, an authenticated attacker can craft a malicious payload to achieve command injection when adding container repositories. The vulnerability has been fixed in v1.3.6.	6.3	More Details
CVE-2023-3528	A vulnerability was found in ThinuTech ThinuCMS 1.5. It has been rated as critical. Affected by this issue is some unknown functionality of the file /category.php. The manipulation of the argument cat_id leads to sql injection. The attack may be launched remotely. The identifier of this vulnerability is VDB-233252.	6.3	More Details
CVE-2023-30659	Improper input validation vulnerability in Transaction prior to SMR Jul-2023 Release 1 allows local attackers to launch privileged activities.	6.2	More Details
CVE-2023-30657	Improper input validation vulnerability in EnhancedAttestationResult prior to SMR Jul-2023 Release 1 allows local attackers to launch privileged activities.	6.2	More Details
CVE-2023-30675	Improper authentication in Samsung Pass prior to version 4.2.03.1 allows local attacker to access stored account information when Samsung Wallet is not installed.	6.2	More Details
CVE-2023-30660	Exposure of Sensitive Information vulnerability in getDefaultChipId in UwbAospAdapterService prior to SMR Jul-2023 Release 1 allows local attackers to access the UWB chipset Identifier.	6.2	More Details

CVE Number	Description	Base Score	Reference
CVE-2023-30661	Exposure of Sensitive Information vulnerability in getChipInfos in UwbAospAdapterService prior to SMR Jul-2023 Release 1 allows local attackers to access the UWB chipset Identifier.	6.2	More Details
CVE-2023-30662	Exposure of Sensitive Information vulnerability in getChipIds in UwbAospAdapterService prior to SMR Jul-2023 Release 1 allows local attackers to access the UWB chipset Identifier.	6.2	More Details
CVE-2023-32627	A floating point exception vulnerability was found in sox, in the read_samples function at sox/src/voc.c:334:18. This flaw can lead to a denial of service.	6.2	More Details
CVE-2023-30642	Improper privilege management vulnerability in Galaxy Themes Service prior to SMR Jul-2023 Release 1 allows local attackers to call privilege function.	6.2	More Details
CVE-2023-35341	Microsoft DirectMusic Information Disclosure Vulnerability	6.2	More Details
CVE-2023-26590	A floating point exception vulnerability was found in sox, in the lsx_aiffstartwrite function at sox/src/aiff.c:622:58. This flaw can lead to a denial of service.	6.2	More Details
CVE-2021-42079	An authenticated administrator is able to prepare an alert that is able to execute an SSRF attack. This is exclusively with POST requests.	6.2	More Details
CVE-2023-3108	A flaw was found in the subsequent get_user_pages_fast in the Linux kernel’s interface for symmetric key cipher algorithms in the skcipher_recvmsg of crypto/algif_skcipher.c function. This flaw allows a local user to crash the system.	6.2	More Details
CVE-2023-29656	An improper authorization vulnerability in Darktrace mobile app (Android) prior to version 6.0.15 allows disabled and low-privilege users to control "antigena" actions(block/unblock traffic) from the mobile application. This vulnerability could create a "shutdown", blocking all ingress or egress traffic in the entire infrastructure where darktrace agents are deployed.	6.1	More Details
CVE-2023-3521	Cross-site Scripting (XSS) - Reflected in GitHub repository fossbilling/fossbilling prior to 0.5.4.	6.1	More Details
CVE-2023-30677	Improper access control vulnerability in Samsung Pass prior to version 4.2.03.1 allows physical attackers to access data of Samsung Pass on a certain state of an unlocked device.	6.1	More Details

CVE Number	Description	Base Score	Reference
CVE-2023-33988	In SAP Enable Now - versions WPB_MANAGER 1.0, WPB_MANAGER_CE 10, WPB_MANAGER_HANA 10, ENABLE_NOW_CONSUMP_DEL 1704, the Content-Security-Policy and X-XSS-Protection response headers are not implemented, allowing an unauthenticated attacker to attempt reflected cross-site scripting, which could result in disclosure or modification of information.	6.1	More Details
CVE-2023-36995	TravianZ through 8.3.4 allows XSS via the Alliance tag/name, the statistics page, the link preferences, the Admin Logs, or the COOKUSR cookie.	6.1	More Details
CVE-2023-36163	Cross Site Scripting vulnerability in IP-DOT BuildaGate v.BuildaGate5 allows a remote attacker to execute arbitrary code via a crafted script to the mc parameter of the URL.	6.1	More Details
CVE-2023-36918	In SAP Enable Now - versions WPB_MANAGER 1.0, WPB_MANAGER_CE 10, WPB_MANAGER_HANA 10, ENABLE_NOW_CONSUMP_DEL 1704, the X-Content-Type-Options response header is not implemented, allowing an unauthenticated attacker to trigger MIME type sniffing, which leads to Cross-Site Scripting, which could result in disclosure or modification of information.	6.1	More Details
CVE-2023-35936	Pandoc is a Haskell library for converting from one markup format to another, and a command-line tool that uses this library. Starting in version 1.13 and prior to version 3.1.4, Pandoc is susceptible to an arbitrary file write vulnerability, which can be triggered by providing a specially crafted image element in the input when generating files using the `--extract-media` option or outputting to PDF format. This vulnerability allows an attacker to create or overwrite arbitrary files on the system ,depending on the privileges of the process running pandoc. It only affects systems that pass untrusted user input to pandoc and allow pandoc to be used to produce a PDF or with the `--extract-media` option. The fix is to unescape the percent-encoding prior to checking that the resource is not above the working directory, and prior to extracting the extension. Some code for checking that the path is below the working directory was flawed in a similar way and has also been fixed. Note that the `--sandbox` option, which only affects IO done by readers and writers themselves, does not block this vulnerability. The vulnerability is patched in pandoc 3.1.4. As a workaround, audit the pandoc command and disallow PDF output and the `--extract-media` option.	6.1	More Details
CVE-2023-34654	taocms <=3.0.2 is vulnerable to Cross Site Scripting (XSS).	6.1	More Details

CVE Number	Description	Base Score	Reference
CVE-2023-36939	Cross-Site Scripting (XSS) vulnerability in Hostel Management System v2.1 allows an attacker to execute arbitrary code via a crafted payload to the search booking field.	6.1	More Details
CVE-2023-23756	Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') vulnerability in advcomsys.com oneVote component for Joomla. It allows XSS Targeting Non-Script Elements.	6.1	More Details
CVE-2023-2853	Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') vulnerability in Softmed SelfPatron allows Reflected XSS.This issue affects SelfPatron : before 2.0.	6.1	More Details
CVE-2023-35978	A vulnerability in ArubaOS could allow an unauthenticated remote attacker to conduct a reflected cross-site scripting (XSS) attack against a user of the web-based management 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.	6.1	More Details
CVE-2023-33335	Cross Site Scripting (XSS) in Sophos Sophos iView (The EOL was December 31st 2020) in grpname parameter that allows arbitrary script to be executed.	6.1	More Details
CVE-2023-1119	The WP-Optimize WordPress plugin before 3.2.13, SrbTransLatin WordPress plugin before 2.4.1 use a third-party library that removes the escaping on some HTML characters, leading to a cross-site scripting vulnerability.	6.1	More Details
CVE-2023-1780	The Companion Sitemap Generator WordPress plugin before 4.5.3 does not sanitise and escape some parameters before outputting them back in pages, leading to Reflected Cross-Site Scripting which could be used against high privilege users such as admin.	6.1	More Details
CVE-2023-3118	The Export All URLs WordPress plugin before 4.6 does not sanitise and escape a parameter before outputting them back in the page, leading to a Reflected Cross-Site Scripting which could be used against high privilege users such as admin	6.1	More Details
CVE-2023-30326	Cross Site Scripting (XSS) vulnerability in username field in /WebContent/WEB-INF/lib/chatbox.jsp in wliang6 ChatEngine commit fded8e710ad59f816867ad47d7fc4862f6502f3e, allows attackers to execute arbitrary code.	6.1	More Details
CVE-2023-36936	Cross-Site Scripting (XSS) vulnerability in PHPGurukul Online Security Guards Hiring System using PHP and MySQL 1.0 allows attackers to execute arbitrary code via a crafted payload to the search booking box.	6.1	More Details

CVE Number	Description	Base Score	Reference
CVE-2020-23452	A cross-site scripting (XSS) vulnerability in Selenium Grid v3.141.59 allows attackers to execute arbitrary web scripts or HTML via a crafted payload injected into the hub parameter under the /grid/console page.	6.1	More Details
CVE-2023-24488	Cross site scripting vulnerability in Citrix ADC and Citrix Gateway in allows and attacker to perform cross site scripting	6.1	More Details
CVE-2023-37153	KodExplorer 4.51 contains a Cross-Site Scripting (XSS) vulnerability in the Description box of the Light App creation feature. An attacker can exploit this vulnerability by injecting XSS syntax into the Description field.	6.1	More Details
CVE-2023-37150	Sourcecodester Online Pizza Ordering System v1.0 has a Cross-site scripting (XSS) vulnerability in "/admin/index.php?page=categories" Category item.	6.1	More Details
CVE-2023-35934	yt-dlp is a command-line program to download videos from video sites. During file downloads, yt-dlp or the external downloaders that yt-dlp employs may leak cookies on HTTP redirects to a different host, or leak them when the host for download fragments differs from their parent manifest's host. This vulnerable behavior is present in yt-dlp prior to 2023.07.06 and nightly 2023.07.06.185519. All native and external downloaders are affected, except for `curl` and `httpie` (version 3.1.0 or later). At the file download stage, all cookies are passed by yt-dlp to the file downloader as a `Cookie` header, thereby losing their scope. This also occurs in yt-dlp's info JSON output, which may be used by external tools. As a result, the downloader or external tool may indiscriminately send cookies with requests to domains or paths for which the cookies are not scoped. yt-dlp version 2023.07.06 and nightly 2023.07.06.185519 fix this issue by removing the `Cookie` header upon HTTP redirects; having native downloaders calculate the `Cookie` header from the cookiejar, utilizing external downloaders' built-in support for cookies instead of passing them as header arguments, disabling HTTP redirectiong if the external downloader does not have proper cookie support, processing cookies passed as HTTP headers to limit their scope, and having a separate field for cookies in the info dict storing more information about scoping Some workarounds are available for those who are unable to upgrade. Avoid using cookies and user authentication methods. While extractors may set custom cookies, these usually do not contain sensitive information. Alternatively, avoid using `--load-info-json`. Or, if authentication is a must: verify the integrity of download links from unknown sources in browser (including redirects) before passing them to yt-dlp; use `curl` as external downloader, since it is not impacted; and/or avoid fragmented formats such as HLS/m3u8, DASH/mpd and ISM.	6.1	More Details

CVE Number	Description	Base Score	Reference
CVE-2023-35937	Metersphere is an open source continuous testing platform. In versions prior to 2.10.2 LTS, some key APIs in Metersphere lack permission checks. This allows ordinary users to execute APIs that can only be executed by space administrators or project administrators. For example, ordinary users can be updated as space administrators. Version 2.10.2 LTS has a patch for this issue.	6.0	More Details
CVE-2023-35874	SAP NetWeaver Application Server ABAP and ABAP Platform - version KRNL64NUC, 7.22, KRNL64NUC 7.22EXT, KRNL64UC 7.22, KRNL64UC 7.22EXT, KRNL64UC 7.53, KERNEL 7.22, KERNEL, 7.53, KERNEL 7.77, KERNEL 7.81, KERNEL 7.85, KERNEL 7.89, KERNEL 7.54, KERNEL 7.92, KERNEL 7.93, under some conditions, performs improper authentication checks for functionalities that require user identity. An attacker can perform malicious actions over the network, extending the scope of impact, causing a limited impact on confidentiality, integrity and availability.	6.0	More Details
CVE-2023-30442	IBM Db2 for Linux, UNIX and Windows (includes Db2 Connect Server) 11.1 and 11.5 federated server is vulnerable to a denial of service as the server may crash when using a specially crafted wrapper using certain options. IBM X-Force ID: 253202.	5.9	More Details
CVE-2023-36748	A vulnerability has been identified in RUGGEDCOM ROX MX5000 (All versions < V2.16.0), RUGGEDCOM ROX MX5000RE (All versions < V2.16.0), RUGGEDCOM ROX RX1400 (All versions < V2.16.0), RUGGEDCOM ROX RX1500 (All versions < V2.16.0), RUGGEDCOM ROX RX1501 (All versions < V2.16.0), RUGGEDCOM ROX RX1510 (All versions < V2.16.0), RUGGEDCOM ROX RX1511 (All versions < V2.16.0), RUGGEDCOM ROX RX1512 (All versions < V2.16.0), RUGGEDCOM ROX RX1524 (All versions < V2.16.0), RUGGEDCOM ROX RX1536 (All versions < V2.16.0), RUGGEDCOM ROX RX5000 (All versions < V2.16.0). The affected devices are configured to offer weak ciphers by default. This could allow an unauthorized attacker in a man-in-the-middle position to read and modify any data passed over to and from the affected device.	5.9	More Details
CVE-2023-30446	IBM Db2 for Linux, UNIX and Windows (includes Db2 Connect Server) 10.5, 11.1, and 11.5 is vulnerable to denial of service with a specially crafted query on certain tables. IBM X-Force ID: 253361 .	5.9	More Details
CVE-2023-34457	MechanicalSoup is a Python library for automating interaction with websites. Starting in version 0.2.0 and prior to version 1.3.0, a malicious web server can read arbitrary files on the client using a `<input type="file" ...>` inside HTML form. All users of MechanicalSoup's form submission are affected, unless they took very specific (and manual) steps to reset HTML form field values. Version 1.3.0 contains a patch for this issue.	5.9	More Details

CVE Number	Description	Base Score	Reference
CVE-2023-1902	The bluetooth HCI host layer logic not clearing a global reference to a state pointer after handling connection events may allow a malicious HCI Controller to cause the use of a dangling reference in the host layer, leading to a crash (DoS) or potential RCE on the Host layer.	5.9	More Details
CVE-2023-1901	The bluetooth HCI host layer logic not clearing a global reference to a semaphore after synchronously sending HCI commands may allow a malicious HCI Controller to cause the use of a dangling reference in the host layer, leading to a crash (DoS) or potential RCE on the Host layer.	5.9	More Details
CVE-2023-0359	A missing nullptr-check in handle_ra_input can cause a nullptr-deref.	5.9	More Details
CVE-2023-30447	IBM Db2 for Linux, UNIX and Windows (includes Db2 Connect Server) 10.5, 11.1, and 11.5 is vulnerable to denial of service with a specially crafted query on certain tables. IBM X-Force ID: 253436.	5.9	More Details
CVE-2023-27540	IBM Watson CP4D Data Stores 4.6.0 does not properly allocate resources without limits or throttling which could allow a remote attacker with information specific to the system to cause a denial of service. IBM X-Force ID: 248924.	5.9	More Details
CVE-2023-30448	IBM DB2 for Linux, UNIX and Windows (includes Db2 Connect Server) 10.5, 11.1, and 11.5 is vulnerable to denial of service with a specially crafted query on certain tables. IBM X-Force ID: 253437.	5.9	More Details
CVE-2022-48509	Race condition vulnerability due to multi-thread access to mutually exclusive resources in Huawei Share. Successful exploitation of this vulnerability may cause the program to exit abnormally.	5.9	More Details
CVE-2023-36917	SAP BusinessObjects Business Intelligence Platform - version 420, 430, allows an unauthorized attacker who had hijacked a user session, to be able to bypass the victim’s old password via brute force, due to unrestricted rate limit for password change functionality. Although the attack has no impact on integrity loss or system availability, this could lead to an attacker to completely takeover a victim’s account.	5.9	More Details

CVE Number	Description	Base Score	Reference
CVE-2023-33868	The number of login attempts is not limited. This could allow an attacker to perform a brute force on HTTP basic authentication.	5.9	More Details
CVE-2023-2538	A CWE-552 "Files or Directories Accessible to External Parties” in the web interface of the Tyan S5552 BMC version 3.00 allows an unauthenticated remote attacker to retrieve the private key of the TLS certificate in use by the BMC via forced browsing. This can then be abused to perform Man-in-the-Middle (MitM) attacks against victims that access the web interface through HTTPS.	5.8	More Details
CVE-2023-34472	AMI SPx contains a vulnerability in the BMC where an Attacker may cause an improper neutralization of CRLF sequences in HTTP Headers. A successful exploit of this vulnerability may lead to a loss of integrity.	5.7	More Details
CVE-2023-30673	Improper validation of integrity check vulnerability in Smart Switch PC prior to version 4.3.23052_1 allows local attackers to delete arbitrary directory using directory junction.	5.5	More Details
CVE-2023-37766	GPAC v2.3-DEV-rev381-g817a848f6-master was discovered to contain a segmentation violation in the gf_isom_remove_user_data function at /lib/libgpac.so.	5.5	More Details
CVE-2023-33174	Windows Cryptographic Information Disclosure Vulnerability	5.5	More Details
CVE-2023-33162	Microsoft Excel Information Disclosure Vulnerability	5.5	More Details
CVE-2023-37765	GPAC v2.3-DEV-rev381-g817a848f6-master was discovered to contain a segmentation violation in the gf_dump_vrml_sffield function at /lib/libgpac.so.	5.5	More Details
CVE-2023-32085	Microsoft PostScript and PCL6 Class Printer Driver Information Disclosure Vulnerability	5.5	More Details
CVE-2023-37174	GPAC v2.3-DEV-rev381-g817a848f6-master was discovered to contain a segmentation violation in the dump_isom_scene function at /mp4box/filedump.c.	5.5	More Details
CVE-2023-30207	A divide by zero issue discovered in Kodi Home Theater Software 19.5 and earlier allows attackers to cause a denial of service via use of crafted mp3 file.	5.5	More Details

CVE Number	Description	Base Score	Reference
CVE-2023-32041	Windows Update Orchestrator Service Information Disclosure Vulnerability	5.5	More Details
CVE-2023-36872	VP9 Video Extensions Information Disclosure Vulnerability	5.5	More Details
CVE-2023-35306	Microsoft PostScript and PCL6 Class Printer Driver Information Disclosure Vulnerability	5.5	More Details
CVE-2020-20118	Buffer Overflow vulnerability in Avast AntiVirus before v.19.7 allows a local attacker to cause a denial of service via a crafted request to the aswSnx.sys driver.	5.5	More Details
CVE-2023-36828	Statamic is a flat-first, Laravel and Git powered content management system. Prior to version 4.10.0, the SVG tag does not sanitize malicious SVG. Therefore, an attacker can exploit this vulnerability to perform cross-site scripting attacks using SVG, even when using the `sanitize` function. Version 4.10.0 contains a patch for this issue.	5.5	More Details
CVE-2023-32040	Microsoft PostScript and PCL6 Class Printer Driver Information Disclosure Vulnerability	5.5	More Details
CVE-2023-32039	Microsoft PostScript and PCL6 Class Printer Driver Information Disclosure Vulnerability	5.5	More Details
CVE-2022-48518	Vulnerability of signature verification in the iaware system being initialized later than the time when the system broadcasts are sent. Successful exploitation of this vulnerability may cause malicious apps to start upon power-on by spoofing the package names of apps in the startup trustlist, which affects system performance.	5.5	More Details
CVE-2023-37767	GPAC v2.3-DEV-rev381-g817a848f6-master was discovered to contain a segmentation violation in the BM_ParseIndexValueReplace function at /lib/libgpac.so.	5.5	More Details
CVE-2023-35324	Microsoft PostScript and PCL6 Class Printer Driver Information Disclosure Vulnerability	5.5	More Details

CVE Number	Description	Base Score	Reference
CVE-2023-3578	A vulnerability classified as critical was found in DedeCMS 5.7.109. Affected by this vulnerability is an unknown functionality of the file co_do.php. The manipulation of the argument rssurl leads to server-side request forgery. The exploit has been disclosed to the public and may be used. The associated identifier of this vulnerability is VDB-233371.	5.5	More Details
CVE-2023-37454	An issue was discovered in the Linux kernel through 6.4.2. A crafted UDF filesystem image causes a use-after-free write operation in the udf_put_super and udf_close_lvid functions in fs/udf/super.c. NOTE: the suse.com reference has a different perspective about this.	5.5	More Details
CVE-2023-25399	A refcounting issue which leads to potential memory leak was discovered in scipy commit 8627df31ab in Py_FindObjects() function. Note: This is disputed as a bug and not a vulnerability. SciPy is not designed to be exposed to untrusted users or data directly.	5.5	More Details
CVE-2023-35326	Windows CDP User Components Information Disclosure Vulnerability	5.5	More Details
CVE-2023-3607	A vulnerability was found in kodbox 1.26. It has been declared as critical. This vulnerability affects the function Execute of the file webconsole.php.txt of the component WebConsole Plug-In. The manipulation leads to os command injection. The exploit has been disclosed to the public and may be used. The identifier of this vulnerability is VDB-233476. NOTE: The vendor was contacted early about this disclosure but did not respond in any way.	5.5	More Details
CVE-2023-24486	A vulnerability has been identified in Citrix Workspace app for Linux that, if exploited, may result in a malicious local user being able to gain access to the Citrix Virtual Apps and Desktops session of another user who is using the same computer from which the ICA session is launched.	5.5	More Details
CVE-2016-15034	A vulnerability was found in Dynacase Webdesk and classified as critical. Affected by this issue is the function freedomrss_search of the file freedomrss_search.php. The manipulation leads to sql injection. Upgrading to version 3.2-20180305 is able to address this issue. The patch is identified as 750a9b35af182950c952faf6ddfdcc50a2b25f8b. It is recommended to upgrade the affected component. VDB-233366 is the identifier assigned to this vulnerability.	5.5	More Details
CVE-2023-37657	TwoNav v2.0.28-20230624 is vulnerable to Cross Site Scripting (XSS).	5.4	More Details

CVE Number	Description	Base Score	Reference
CVE-2023-36970	A Cross-site scripting (XSS) vulnerability in CMS Made Simple v2.2.17 allows remote attackers to inject arbitrary web script or HTML via the File Upload function.	5.4	More Details
CVE-2023-37658	fast-poster v2.15.0 is vulnerable to Cross Site Scripting (XSS). File upload check binary of img, but without strictly check file suffix at /server/fast.py -> ApiUploadHandler.post causes stored XSS	5.4	More Details
CVE-2023-24421	Cross-Site Request Forgery (CSRF) vulnerability in WP Engine PHP Compatibility Checker plugin <= 1.5.2 versions.	5.4	More Details
CVE-2023-3620	Cross-site Scripting (XSS) - Stored in GitHub repository amauric/tarteaucitron.js prior to v1.13.1.	5.4	More Details
CVE-2023-22673	Cross-Site Request Forgery (CSRF) vulnerability in MageNet Website Monetization by MageNet plugin <= 1.0.29.1 versions.	5.4	More Details
CVE-2023-24395	Cross-Site Request Forgery (CSRF) vulnerability in Scott Paterson Contact Form 7 Redirect & Thank You Page plugin <= 1.0.3 versions.	5.4	More Details
CVE-2023-24405	Cross-Site Request Forgery (CSRF) vulnerability in Scott Paterson Contact Form 7 – PayPal & Stripe Add-on plugin <= 1.9.3 versions.	5.4	More Details
CVE-2023-37122	A stored cross-site scripting (XSS) vulnerability in Bagecms v3.1.0 allows attackers to execute arbitrary web scripts or HTML via a crafted payload injected into the Custom Settings module.	5.4	More Details
CVE-2023-3532	Cross-site Scripting (XSS) - Stored in GitHub repository outline/outline prior to 0.70.1.	5.4	More Details
CVE-2023-30963	A security defect was discovered in Foundry Frontend which enabled users to perform Stored XSS attacks in Slate if Foundry's CSP were to be bypassed. This defect was resolved with the release of Foundry Frontend 6.229.0. The service was rolled out to all affected Foundry instances. No further intervention is required.	5.4	More Details
CVE-2023-27225	A cross-site scripting (XSS) vulnerability in User Registration & Login and User Management System with Admin Panel v3 allows attackers to execute arbitrary web scripts or HTML via a crafted payload injected into the first and last name field.	5.4	More Details

CVE Number	Description	Base Score	Reference
CVE-2023-28986	Cross-Site Request Forgery (CSRF) vulnerability in wp.Insider, wpaffiliatemgr Affiliates Manager plugin <= 2.9.20 versions.	5.4	More Details
CVE-2023-3552	Improper Encoding or Escaping of Output in GitHub repository nilsteampassnet/teampass prior to 3.0.10.	5.4	More Details
CVE-2023-26138	All versions of the package drogonframework/drogon are vulnerable to CRLF Injection when untrusted user input is used to set request headers in the addHeader function. An attacker can add the \r\n (carriage return line feeds) characters and inject additional headers in the request sent.	5.4	More Details
CVE-2023-20133	A vulnerability in the web interface of Cisco Webex Meetings could allow an authenticated, remote attacker to conduct a stored cross-site scripting (XSS) attack against a user of the interface. This vulnerability exists because of insufficient validation of user-supplied input in Webex Events (classic) programs, email templates, and survey questions. An attacker could exploit this vulnerability by persuading a user to click a malicious link. A successful exploit could allow the attacker to execute arbitrary script code in the context of the affected interface or access sensitive, browser-based information.	5.4	More Details
CVE-2023-34197	Zoho ManageEngine ServiceDesk Plus before 14202, ServiceDesk Plus MSP before 14300, and SupportCenter Plus before 14300 have a privilege escalation vulnerability in the Release module that allows unprivileged users to access the Reminders of a release ticket and make modifications.	5.4	More Details
CVE-2023-3565	Cross-site Scripting (XSS) - Generic in GitHub repository nilsteampassnet/teampass prior to 3.0.10.	5.4	More Details
CVE-2023-37308	Zoho ManageEngine ADAudit Plus before 7100 allows XSS via the username field.	5.4	More Details
CVE-2023-35948	Novu provides an API for sending notifications through multiple channels. Versions prior to 0.16.0 contain an open redirect vulnerability in the "Sign In with GitHub" functionality of Novu's open-source repository. It could have allowed an attacker to force a victim into opening a malicious URL and thus, potentially log into the repository under the victim's account gaining full control of the account. This vulnerability only affected the Novu Cloud and Open-Source deployments if the user manually enabled the GitHub OAuth on their self-hosted instance of Novu. Users should upgrade to version 0.16.0 to receive a patch.	5.4	More Details

CVE Number	Description	Base Score	Reference
CVE-2023-29998	A Cross-site scripting (XSS) vulnerability in the content editor in Gis3W g3w-suite 3.5 allows remote authenticated users to inject arbitrary web script or HTML and gain privileges via the description parameter.	5.4	More Details
CVE-2023-32052	Microsoft Power Apps (online) Spoofing Vulnerability	5.4	More Details
CVE-2023-36375	Cross Site Scripting vulnerability in Hostel Management System v2.1 allows an attacker to execute arbitrary code via a crafted payload to the Guardian name, Guardian relation, complimentary address, city, permanent address, and city parameters in the Book Hostel & Room Details page.	5.4	More Details
CVE-2023-37124	A stored cross-site scripting (XSS) vulnerability in the Site Setup module of SEACMS v12.1 allows attackers to execute arbitrary web scripts or HTML via a crafted payload.	5.4	More Details
CVE-2023-23993	Cross-Site Request Forgery (CSRF) vulnerability in LionScripts.Com LionScripts: IP Blocker Lite plugin <= 11.1.1 versions.	5.4	More Details
CVE-2023-28995	Cross-Site Request Forgery (CSRF) vulnerability in Keith Solomon Configurable Tag Cloud (CTC) plugin <= 5.2 versions.	5.4	More Details
CVE-2023-37135	A stored cross-site scripting (XSS) vulnerability in the Image Upload module of eyoucms v1.6.3 allows attackers to execute arbitrary web scripts or HTML via a crafted payload.	5.4	More Details
CVE-2023-36691	Cross-Site Request Forgery (CSRF) vulnerability in Albert Peschar WebwinkelKeur plugin <= 3.24 versions.	5.4	More Details
CVE-2023-35774	Cross-Site Request Forgery (CSRF) vulnerability in LWS LWS Tools plugin <= 2.4.1 versions.	5.4	More Details
CVE-2023-34015	Cross-Site Request Forgery (CSRF) vulnerability in PI Websolution Conditional shipping & Advanced Flat rate shipping rates / Flexible shipping for WooCommerce shipping plugin <= 1.6.4.4 versions.	5.4	More Details
CVE-2023-37392	Cross-Site Request Forgery (CSRF) vulnerability in Deepak Anand WP Dummy Content Generator plugin <= 2.3.0 versions.	5.4	More Details

CVE Number	Description	Base Score	Reference
CVE-2023-2964	The Simple Iframe WordPress plugin before 1.2.0 does not properly validate one of its WordPress block attribute's content, which may allow users whose role is at least that of a contributor to conduct Stored Cross-Site Scripting attacks.	5.4	More Details
CVE-2023-37136	A stored cross-site scripting (XSS) vulnerability in the Basic Website Information module of eyoucms v1.6.3 allows attackers to execute arbitrary web scripts or HTML via a crafted payload.	5.4	More Details
CVE-2023-36462	Mastodon is a free, open-source social network server based on ActivityPub. Starting in version 2.6.0 and prior to versions 3.5.9, 4.0.5, and 4.1.3, an attacker can craft a verified profile link using specific formatting to conceal arbitrary parts of the link, enabling it to appear to link to a different URL altogether. The link is visually misleading, but clicking on it will reveal the actual link. This can still be used for phishing, though, similar to IDN homograph attacks. Versions 3.5.9, 4.0.5, and 4.1.3 contain a patch for this issue.	5.4	More Details
CVE-2023-3531	Cross-site Scripting (XSS) - Stored in GitHub repository nilsteampassnet/teampass prior to 3.0.10.	5.4	More Details
CVE-2023-37391	Cross-Site Request Forgery (CSRF) vulnerability in WPMobilePack.Com WordPress Mobile Pack – Mobile Plugin for Progressive Web Apps & Hybrid Mobile Apps plugin <= 3.4.1 versions.	5.4	More Details
CVE-2023-36687	Cross-Site Request Forgery (CSRF) vulnerability in Andrea Tarantini Menubar plugin <= 5.8.2 versions.	5.4	More Details
CVE-2023-30322	Cross Site Scripting (XSS) vulnerability in username field in /src/chatbotapp/chatWindow.java in Payatu ChatEngine v.1.0, allows attackers to execute arbitrary code.	5.4	More Details
CVE-2023-25706	Cross-Site Request Forgery (CSRF) vulnerability in Pagup WordPress Robots.Txt optimization plugin <= 1.4.5 versions.	5.4	More Details
CVE-2023-2529	The Enable SVG Uploads WordPress plugin through 2.1.5 does not sanitise uploaded SVG files, which could allow users with a role as low as Author to upload a malicious SVG containing XSS payloads.	5.4	More Details
CVE-2023-37133	A stored cross-site scripting (XSS) vulnerability in the Column management module of eyoucms v1.6.3 allows attackers to execute arbitrary web scripts or HTML via a crafted payload.	5.4	More Details

CVE Number	Description	Base Score	Reference
CVE-2023-37132	A stored cross-site scripting (XSS) vulnerability in the custom variables module of eyoucms v1.6.3 allows attackers to execute arbitrary web scripts or HTML via a crafted payload.	5.4	More Details
CVE-2023-37125	A stored cross-site scripting (XSS) vulnerability in the Management Custom label module of SEACMS v12.1 allows attackers to execute arbitrary web scripts or HTML via a crafted payload.	5.4	More Details
CVE-2023-35781	Cross-Site Request Forgery (CSRF) vulnerability in LWS Cleaner plugin <= 2.3.0 versions.	5.4	More Details
CVE-2023-37134	A stored cross-site scripting (XSS) vulnerability in the Basic Information module of eyoucms v1.6.3 allows attackers to execute arbitrary web scripts or HTML via a crafted payload.	5.4	More Details
CVE-2023-35698	Observable Response Discrepancy in the SICK ICR890-4 could allow a remote attacker to identify valid usernames for the FTP server from the response given during a failed login attempt.	5.3	More Details
CVE-2023-35697	Improper Restriction of Excessive Authentication Attempts in the SICK ICR890-4 could allow a remote attacker to brute-force user credentials.	5.3	More Details
CVE-2022-22302	A clear text storage of sensitive information (CWE-312) vulnerability in both FortiGate version 6.4.0 through 6.4.1, 6.2.0 through 6.2.9 and 6.0.0 through 6.0.13 and FortiAuthenticator version 5.5.0 and all versions of 6.1 and 6.0 may allow a local unauthorized party to retrieve the Fortinet private keys used to establish secure communication with both Apple Push Notification and Google Cloud Messaging services, via accessing the files on the filesystem.	5.3	More Details
CVE-2022-48521	An issue was discovered in OpenDKIM through 2.10.3, and 2.11.x through 2.11.0-Beta2. It fails to keep track of ordinal numbers when removing fake Authentication-Results header fields, which allows a remote attacker to craft an e-mail message with a fake sender address such that programs that rely on Authentication-Results from OpenDKIM will treat the message as having a valid DKIM signature when in fact it has none.	5.3	More Details
CVE-2023-35979	There is an unauthenticated buffer overflow vulnerability in the process controlling the ArubaOS web-based management interface. Successful exploitation of this vulnerability results in a Denial-of-Service (DoS) condition affecting the web-based management interface of the controller.	5.3	More Details

CVE Number	Description	Base Score	Reference
CVE-2023-35863	In MADEFORNET HTTP Debugger through 9.12, the Windows service does not set the seclevel registry key before launching the driver. Thus, it is possible for an unprivileged application to obtain a handle to the NetFilterSDK wrapper before the service obtains exclusive access.	5.3	More Details
CVE-2023-35699	Cleartext Storage on Disk in the SICK ICR890-4 could allow an unauthenticated attacker with local access to the device to disclose sensitive information by accessing a SD card.	5.3	More Details
CVE-2023-3219	The EventON WordPress plugin before 2.1.2 does not validate that the event_id parameter in its eventon_ics_download ajax action is a valid Event, allowing unauthenticated visitors to access any Post (including unpublished or protected posts) content via the ics export functionality by providing the numeric id of the post.	5.3	More Details
CVE-2023-30666	Improper input validation vulnerability in DoOemImeiSetPreconfig in libsec-ril prior to SMR Jul-2023 Release 1 allows local attackers to cause an Out-Of-Bounds write.	5.3	More Details
CVE-2023-3529	A vulnerability classified as problematic has been found in Rotem Dynamics Rotem CRM up to 20230729. This affects an unknown part of the file /LandingPages/api/otp/send?id=[ID][ampersand]method=sms of the component OTP URI Interface. The manipulation leads to information exposure through discrepancy. It is possible to initiate the attack remotely. The identifier VDB-233253 was assigned to this vulnerability. NOTE: The vendor was contacted early about this disclosure but did not respond in any way.	5.3	More Details
CVE-2023-3336	TN-5900 Series version 3.3 and prior versions is vulnearble to user enumeration vulnerability. The vulnerability may allow a remote attacker to determine whether a user is valid during password recovery through the web login page and enable a brute force attack with valid users.	5.3	More Details
CVE-2023-29256	IBM Db2 for Linux, UNIX and Windows (includes Db2 Connect Server) 10.5, 11.1, and 11.5 is vulnerable to an information disclosure due to improper privilege management when certain federation features are used. IBM X-Force ID: 252046.	5.3	More Details
CVE-2023-30663	Improper input validation vulnerability in OemPersonalizationSetLock in libsec-ril prior to SMR Jul-2023 Release 1 allows local attackers to cause an Out-Of-Bounds write.	5.3	More Details
CVE-2023-30956	A security defect was identified in Foundry Comments that enabled a user to discover the contents of an attachment submitted to another comment if they knew the internal UUID of the target attachment. This defect was resolved with the release of Foundry Comments 2.267.0.	5.3	More Details

CVE Number	Description	Base Score	Reference
CVE-2023-31194	An improper array index validation vulnerability exists in the GraphPlanar::Write functionality of Diagon v1.0.139. A specially crafted markdown file can lead to memory corruption. A victim would need to open a malicious file to trigger this vulnerability.	5.3	More Details
CVE-2023-1672	A race condition exists in the Tang server functionality for key generation and key rotation. This flaw results in a small time window where Tang private keys become readable by other processes on the same host.	5.3	More Details
CVE-2023-33201	Bouncy Castle For Java before 1.74 is affected by an LDAP injection vulnerability. The vulnerability only affects applications that use an LDAP CertStore from Bouncy Castle to validate X.509 certificates. During the certificate validation process, Bouncy Castle inserts the certificate's Subject Name into an LDAP search filter without any escaping, which leads to an LDAP injection vulnerability.	5.3	More Details
CVE-2023-35373	Mono Authenticode Validation Spoofing Vulnerability	5.3	More Details
CVE-2023-3456	Vulnerability of kernel raw address leakage in the hang detector module. Successful exploitation of this vulnerability may affect service confidentiality.	5.3	More Details
CVE-2023-37238	Vulnerability of apps' permission to access a certain API being incompletely verified in the wireless projection module. Successful exploitation of this vulnerability may affect some wireless projection features.	5.3	More Details
CVE-2023-33008	Deserialization of Untrusted Data vulnerability in Apache Software Foundation Apache Johnzon. A malicious attacker can craft up some JSON input that uses large numbers (numbers such as 1e20000000) that Apache Johnzon will deserialize into BigDecimal and maybe use numbers too large which may result in a slow conversion (Denial of service risk). Apache Johnzon 1.2.21 mitigates this by setting a scale limit of 1000 (by default) to the BigDecimal. This issue affects Apache Johnzon: through 1.2.20.	5.3	More Details
CVE-2023-31405	SAP NetWeaver AS for Java - versions ENGINEAPI 7.50, SERVERCORE 7.50, J2EE-APPS 7.50, allows an unauthenticated attacker to craft a request over the network which can result in unwarranted modifications to a system log without user interaction. There is no ability to view any information or any effect on availability.	5.3	More Details

CVE Number	Description	Base Score	Reference
CVE-2023-2796	The EventON WordPress plugin before 2.1.2 lacks authentication and authorization in its eventon_ics_download ajax action, allowing unauthenticated visitors to access private and password protected Events by guessing their numeric id.	5.3	More Details
CVE-2023-36919	In SAP Enable Now - versions WPB_MANAGER 1.0, WPB_MANAGER_CE 10, WPB_MANAGER_HANA 10, ENABLE_NOW_CONSUMP_DEL 1704, the Referrer-Policy response header is not implemented, allowing an unauthenticated attacker to obtain referrer details, resulting in information disclosure.	5.3	More Details
CVE-2023-23348	HCL Launch could disclose sensitive information if a manual edit of a configuration file has been performed.	5.1	More Details
CVE-2023-30678	Potential zip path traversal vulnerability in Calendar application prior to version 12.4.07.15 in Android 13 allows attackers to write arbitrary file.	5.1	More Details
CVE-2023-30667	Improper access control in Audio system service prior to SMR Jul-2023 Release 1 allows attacker to send broadcast with system privilege.	5.1	More Details
CVE-2023-35890	IBM WebSphere Application Server 8.5 and 9.0 could provide weaker than expected security, caused by the improper encoding in a local configuration file. IBM X-Force ID: 258637.	5.1	More Details
CVE-2023-30607	icingaweb2-module-jira provides integration with Atlassian Jira. Starting in version 1.3.0 and prior to version 1.3.2, template and field configuration forms perform the deletion action before user input is validated, including the cross site request forgery token. This issue is fixed in version 1.3.2. There are no known workarounds.	5.0	More Details
CVE-2023-37280	Pimcore Admin Classic Bundle provides a Backend UI for Pimcore based on the ExtJS framework. An admin who has not setup two factor authentication before is vulnerable for this attack, without need for any form of privilege, causing the application to execute arbitrary scripts/HTML content. This vulnerability has been patched in version 1.0.3.	5.0	More Details
CVE-2023-1183	A flaw was found in the Libreoffice package. An attacker can craft an odb containing a "database/script" file with a SCRIPT command where the contents of the file could be written to a new file whose location was determined by the attacker.	5.0	More Details

CVE Number	Description	Base Score	Reference
CVE-2023-35887	Exposure of Sensitive Information to an Unauthorized Actor vulnerability in Apache Software Foundation Apache MINA. In SFTP servers implemented using Apache MINA SSHD that use a RootedFileSystem, logged users may be able to discover "exists/does not exist" information about items outside the rooted tree via paths including parent navigation ("..") beyond the root, or involving symlinks. This issue affects Apache MINA: from 1.0 before 2.10. Users are recommended to upgrade to 2.10	5.0	More Details
CVE-2023-35786	Zoho ManageEngine ADManager Plus before 7183 allows admin users to exploit an XXE issue to view files.	4.9	More Details
CVE-2023-36924	While using a specific function, SAP ERP Defense Forces and Public Security - versions 600, 603, 604, 605, 616, 617, 618, 802, 803, 804, 805, 806, 807, allows an authenticated attacker with admin privileges to write arbitrary data to the syslog file. On successful exploitation, an attacker could modify all the syslog data causing a complete compromise of integrity of the application.	4.9	More Details
CVE-2023-2578	The Buy Me a Coffee WordPress plugin before 3.7 does not sanitise and escape some of its settings, which could allow high privilege users such as admin to perform Stored Cross-Site Scripting attacks even when the unfiltered_html capability is disallowed (for example in multisite setup).	4.8	More Details
CVE-2023-3129	The URL Shortify WordPress plugin before 1.7.0 does not sanitise and escape some of its settings, which could allow high privilege users such as admin to perform Stored Cross-Site Scripting attacks even when the unfiltered_html capability is disallowed (for example in multisite setup)	4.8	More Details
CVE-2023-2028	The Call Now Accessibility Button WordPress plugin before 1.1 does not properly sanitize some of its settings, which could allow high-privilege users to perform Stored Cross-Site Scripting (XSS) attacks even when the unfiltered_html capability is disallowed (for example in multisite setup).	4.8	More Details
CVE-2023-2029	The PrePost SEO WordPress plugin through 3.0 does not properly sanitize some of its settings, which could allow high-privilege users to perform Stored Cross-Site Scripting (XSS) attacks even when the unfiltered_html capability is disallowed (for example in multisite setup)	4.8	More Details
CVE-2023-2635	The Call Now Accessibility Button WordPress plugin before 1.1 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 Number	Description	Base Score	Reference
CVE-2023-37061	Chamilo 1.11.x up to 1.11.20 allows users with an admin privilege account to insert XSS in the languages management section.	4.8	More Details
CVE-2023-2709	The AN_GradeBook WordPress plugin through 5.0.1 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-2023-37190	A stored cross-site scripting (XSS) vulnerability in Issabel issabel-pbx v.4.0.0-6 allows attackers to execute arbitrary web scripts or HTML via a crafted payload injected into the Virtual Fax Name and Caller ID Name parameters under the New Virtual Fax feature.	4.8	More Details
CVE-2023-37189	A stored cross site scripting (XSS) vulnerability in index.php?menu=billing_rates of Issabel PBX version 4 allows attackers to execute arbitrary web scripts or HTML via a crafted payload entered into the Name or Prefix fields under the Create New Rate module.	4.8	More Details
CVE-2023-2967	The TinyMCE Custom Styles WordPress plugin before 1.1.4 does not sanitise and escape some of its settings, which could allow high privilege users such as admin to perform Stored Cross-Site Scripting attacks even when the unfiltered_html capability is disallowed (for example in multisite setup).	4.8	More Details
CVE-2023-37191	A stored cross-site scripting (XSS) vulnerability in Issabel issabel-pbx v.4.0.0-6 allows attackers to execute arbitrary web scripts or HTML via a crafted payload injected into the Group and Description parameters.	4.8	More Details
CVE-2023-2026	The Image Protector WordPress plugin through 1.1 does not properly sanitize some of its settings, which could allow high-privilege users to perform Stored Cross-Site Scripting (XSS) attacks even when the unfiltered_html capability is disallowed (for example in multisite setup).	4.8	More Details
CVE-2023-3175	The AI ChatBot WordPress plugin before 4.6.1 does not adequately escape some settings, allowing high-privilege users such as admin to perform Cross-Site Scripting attacks even when the unfiltered_html capability is disallowed.	4.8	More Details
CVE-2023-3225	The Float menu WordPress plugin before 5.0.3 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 Number	Description	Base Score	Reference
CVE-2023-32000	A Cross-Site Scripting (XSS) vulnerability found in UniFi Network (Version 7.3.83 and earlier) allows a malicious actor with Site Administrator credentials to escalate privileges by persuading an Administrator to visit a malicious web page.	4.8	More Details
CVE-2023-37067	Chamilo 1.11.x up to 1.11.20 allows users with admin privilege account to insert XSS in the classes/usergroups management section.	4.8	More Details
CVE-2023-37066	Chamilo 1.11.x up to 1.11.20 allows users with admin privilege account to insert XSS in the skills wheel.	4.8	More Details
CVE-2023-37065	Chamilo 1.11.x up to 1.11.20 allows users with admin privilege account to insert XSS in the session category management section.	4.8	More Details
CVE-2023-37064	Chamilo 1.11.x up to 1.11.20 allows users with admin privilege account to insert XSS in the extra fields management section.	4.8	More Details
CVE-2023-36940	Cross Site Scripting (XSS) vulnerability in PHPGurukul Online Fire Reporting System Using PHP and MySQL v.1.2 allows attackers to execute arbitrary code via a crafted payload injected into the search field.	4.8	More Details
CVE-2023-37063	Chamilo 1.11.x up to 1.11.20 allows users with admin privilege account to insert XSS in the careers & promotions management section.	4.8	More Details
CVE-2023-37062	Chamilo 1.11.x up to 1.11.20 allows users with admin privilege account to insert XSS in the course categories' definition.	4.8	More Details
CVE-2023-36376	Cross-Site Scripting (XSS) vulnerability in Hostel Management System v.2.1 allows attackers to execute arbitrary web scripts or HTML via a crafted payload injected into the add course section.	4.8	More Details
CVE-2023-3608	A vulnerability was found in Ruijie BCR810W 2.5.10. It has been rated as critical. This issue affects some unknown processing of the component Tracert Page. The manipulation leads to os command injection. The attack may be initiated remotely. The exploit has been disclosed to the public and may be used. The identifier VDB-233477 was assigned to this vulnerability. NOTE: The vendor was contacted early about this disclosure but did not respond in any way.	4.7	More Details

CVE Number	Description	Base Score	Reference
CVE-2021-33798	A null pointer dereference was found in libpano13, version libpano13-2.9.20. The flow allows attackers to cause a denial of service and potential code execute via a crafted file.	4.7	More Details
CVE-2023-24496	Cross-site scripting (xss) vulnerabilities exist in the requestHandlers.js detail_device functionality of Milesight VPN v2.0.2. A specially-crafted HTTP request can lead to arbitrary Javascript code injection. An attacker can send an HTTP request to trigger these vulnerabilities.This XSS is exploited through the name field of the database.	4.7	More Details
CVE-2023-24497	Cross-site scripting (xss) vulnerabilities exist in the requestHandlers.js detail_device functionality of Milesight VPN v2.0.2. A specially-crafted HTTP request can lead to arbitrary Javascript code injection. An attacker can send an HTTP request to trigger these vulnerabilities.This XSS is exploited through the remote_subnet field of the database	4.7	More Details
CVE-2023-29156	DroneScout ds230 Remote ID receiver from BlueMark Innovations is affected by an information loss vulnerability through traffic injection. An attacker can exploit this vulnerability by injecting, at the right times, spoofed Open Drone ID (ODID) messages which force the DroneScout ds230 Remote ID receiver to drop real Remote ID (RID) information and, instead, generate and transmit JSON encoded MQTT messages containing crafted RID information. Consequently, the MQTT broker, typically operated by a system integrator, will have no access to the drones' real RID information. This issue affects DroneScout ds230 in default configuration from firmware version 20211210-1627 through 20230329-1042.	4.7	More Details
CVE-2023-3520	Sensitive Cookie in HTTPS Session Without 'Secure' Attribute in GitHub repository it-novum/openitcockpit prior to 4.6.6.	4.6	More Details
CVE-2023-37453	An issue was discovered in the USB subsystem in the Linux kernel through 6.4.2. There is an out-of-bounds and crash in read_descriptors in drivers/usb/core/sysfs.c.	4.6	More Details
CVE-2023-30676	Improper access control vulnerability in Samsung Pass prior to version 4.2.03.1 allows physical attackers to access data of Samsung Pass.	4.6	More Details

CVE Number	Description	Base Score	Reference
CVE-2023-33992	The SAP BW BICS communication layer in SAP Business Warehouse and SAP BW/4HANA - version SAP_BW 730, SAP_BW 731, SAP_BW 740, SAP_BW 730, SAP_BW 750, DW4CORE 100, DW4CORE 200, DW4CORE 300, may expose unauthorized cell values to the data response. To be able to exploit this, the user still needs authorizations on the query as well as on the keyfigure/measure level. The missing check only affects the data level.	4.5	More Details
CVE-2023-30665	Improper input validation vulnerability in OnOemServiceMode in libsec-ril prior to SMR Jul-2023 Release 1 allows local attackers to cause an Out-Of-Bounds read.	4.4	More Details
CVE-2023-3515	Open Redirect in GitHub repository go-gitea/gitea prior to 1.19.4.	4.4	More Details
CVE-2023-23997	Cross-Site Request Forgery (CSRF) vulnerability in Dave Jesch Database Collation Fix plugin <= 1.2.7 versions.	4.3	More Details
CVE-2023-33165	Microsoft SharePoint Server Security Feature Bypass Vulnerability	4.3	More Details
CVE-2023-23731	Cross-Site Request Forgery (CSRF) vulnerability in HasTheme WishSuite plugin <= 1.3.3 versions.	4.3	More Details
CVE-2023-23704	Cross-Site Request Forgery (CSRF) vulnerability in Pixelgrade Comments Ratings plugin <= 1.1.6 versions.	4.3	More Details
CVE-2023-23869	Cross-Site Request Forgery (CSRF) vulnerability in Amit Agarwal Google XML Sitemap for Mobile plugin <= 1.6.1 versions.	4.3	More Details
CVE-2023-23803	Cross-Site Request Forgery (CSRF) vulnerability in HasThemes JustTables plugin <= 1.4.9 versions.	4.3	More Details
CVE-2023-23791	Cross-Site Request Forgery (CSRF) vulnerability in HasThemes HT Menu plugin <= 1.2.1 versions.	4.3	More Details
CVE-2023-23792	Cross-Site Request Forgery (CSRF) vulnerability in HasThemes Swatchly plugin <= 1.2.0 versions.	4.3	More Details

CVE Number	Description	Base Score	Reference
CVE-2023-30960	A security defect was discovered in Foundry job-tracker that enabled users to query metadata related to builds on resources they did not have access to. This defect was resolved with the release of job-tracker 4.645.0. The service was rolled out to all affected Foundry instances. No further intervention is required.	4.3	More Details
CVE-2023-3580	Improper Handling of Additional Special Element in GitHub repository squidex/squidex prior to 7.4.0.	4.3	More Details
CVE-2023-3579	A vulnerability, which was classified as problematic, has been found in HadSky 7.11.8. Affected by this issue is some unknown functionality of the component User Handler. The manipulation leads to cross-site request forgery. The attack may be launched remotely. The exploit has been disclosed to the public and may be used. The identifier of this vulnerability is VDB-233372.	4.3	More Details
CVE-2023-3131	The MStore API WordPress plugin before 3.9.7 does not secure most of its AJAX actions by implementing privilege checks, nonce checks, or a combination of both.	4.3	More Details
CVE-2023-20180	A vulnerability in the web interface of Cisco Webex Meetings could allow an unauthenticated, remote attacker to conduct a cross-site request forgery (CSRF) attack on an affected system. This vulnerability is due to insufficient CSRF protections for the web interface on an affected system. An attacker could exploit this vulnerability by persuading a user of the interface to click a malicious link. A successful exploit could allow the attacker to perform arbitrary actions. These actions could include joining meetings and scheduling training sessions.	4.3	More Details
CVE-2023-25468	Cross-Site Request Forgery (CSRF) vulnerability in Reservation.Studio Reservation.Studio widget plugin <= 1.0.11 versions.	4.3	More Details
CVE-2023-22694	Cross-Site Request Forgery (CSRF) vulnerability in Arian Khosravi, Norik Davtian BigContact Contact Page plugin <= 1.5.8 versions.	4.3	More Details
CVE-2023-22695	Cross-Site Request Forgery (CSRF) vulnerability in Hiroaki Miyashita Custom Field Template plugin <= 2.5.8 versions.	4.3	More Details
CVE-2023-35912	Cross-Site Request Forgery (CSRF) vulnerability in WP Zone Potent Donations for WooCommerce plugin <= 1.1.9 versions.	4.3	More Details

CVE Number	Description	Base Score	Reference
CVE-2023-23487	IBM Db2 for Linux, UNIX and Windows (includes Db2 Connect Server) 11.1 and 11.5 is vulnerable to insufficient audit logging. IBM X-Force ID: 245918.	4.3	More Details
CVE-2023-23787	Cross-Site Request Forgery (CSRF) vulnerability in Premmerce Premmerce Redirect Manager plugin <= 1.0.9 versions.	4.3	More Details
CVE-2023-2495	The Greeklish-permalink WordPress plugin through 3.3 does not implement correct authorization or nonce checks in the cyrtrans_ajax_old AJAX action, allowing unauthenticated and low-privilege users to trigger the plugin's functionality to change Post slugs either directly or through CSRF.	4.3	More Details
CVE-2023-28989	Cross-Site Request Forgery (CSRF) vulnerability in weDevs Happy Addons for Elementor plugin <= 3.8.2 versions.	4.3	More Details
CVE-2023-23804	Cross-Site Request Forgery (CSRF) vulnerability in HasThemes HT Feed plugin <= 1.2.7 versions.	4.3	More Details
CVE-2023-25478	Cross-Site Request Forgery (CSRF) vulnerability in Jason Rouet Weather Station plugin <= 3.8.12 versions.	4.3	More Details
CVE-2023-25051	Cross-Site Request Forgery (CSRF) vulnerability in Denishua Comment Reply Notification plugin <= 1.4 versions.	4.3	More Details
CVE-2022-45823	Cross-Site Request Forgery (CSRF) vulnerability in GalleryPlugins Video Contest WordPress plugin <= 3.2 versions.	4.3	More Details
CVE-2023-25487	Cross-Site Request Forgery (CSRF) vulnerability in Pixelgrade PixTypes plugin <= 1.4.14 versions.	4.3	More Details
CVE-2023-32104	Cross-Site Request Forgery (CSRF) vulnerability in Mark Tilly MyCurator Content Curation plugin <= 3.74 versions.	4.3	More Details
CVE-2023-30641	Improper access control vulnerability in Settings prior to SMR Jul-2023 Release 1 allows physical attacker to use restricted user profile to access device owner's google account data.	4.3	More Details

CVE Number	Description	Base Score	Reference
CVE-2023-30640	Improper access control vulnerability in PersonaManagerService prior to SMR Jul-2023 Release 1 allows local attackers to change confiugration.	4.3	More Details
CVE-2023-1298	ServiceNow has released upgrades and patches that address a Reflected Cross-Site scripting (XSS) vulnerability that was identified in the ServiceNow Polaris Layout. This vulnerability would enable an authenticated user to inject arbitrary scripts.	4.3	More Details
CVE-2020-8934	The Site Kit by Google plugin for WordPress is vulnerable to Sensitive Information Disclosure in versions up to, and including, 1.8.0 This is due to the lack of capability checks on the admin_enqueue_scripts action which displays the connection key. This makes it possible for authenticated attackers with any level of access obtaining owner access to a site in the Google Search Console. We recommend upgrading to V1.8.1 or above.	4.3	More Details
CVE-2023-36522	Cross-Site Request Forgery (CSRF) vulnerability in WePupil Quiz Expert plugin <= 1.5.0 versions.	4.3	More Details
CVE-2023-35773	Cross-Site Request Forgery (CSRF) vulnerability in Danny Hearnah - ChubbyNinjaa Template Debugger plugin <= 3.1.2 versions.	4.3	More Details
CVE-2023-35091	Cross-Site Request Forgery (CSRF) vulnerability in StoreApps Stock Manager for WooCommerce plugin <= 2.10.0 versions.	4.3	More Details
CVE-2023-35044	Cross-Site Request Forgery (CSRF) vulnerability in Drew Phillips Securimage-WP plugin <= 3.6.16 versions.	4.3	More Details
CVE-2023-34029	Cross-Site Request Forgery (CSRF) vulnerability in Prem Tiwari Disable WordPress Update Notifications and auto-update Email Notifications plugin <= 2.3.3 versions.	4.3	More Details
CVE-2023-35913	Cross-Site Request Forgery (CSRF) vulnerability in OOPSpam OOPSpam Anti-Spam plugin <= 1.1.44 versions.	4.3	More Details
CVE-2023-23897	Cross-Site Request Forgery (CSRF) vulnerability in Ozette Plugins Simple Mobile URL Redirect plugin <= 1.7.2 versions.	4.3	More Details

CVE Number	Description	Base Score	Reference
CVE-2023-35780	Cross-Site Request Forgery (CSRF) vulnerability in Andy Whalen Galleria plugin <= 1.0.3 versions.	4.3	More Details
CVE-2023-35778	Cross-Site Request Forgery (CSRF) vulnerability in Neha Goel Recent Posts Slider plugin <= 1.1 versions.	4.3	More Details
CVE-2023-36517	Cross-Site Request Forgery (CSRF) vulnerability in Kevon Adonis WP Abstracts plugin <= 2.6.2 versions.	4.3	More Details
CVE-2023-36693	Cross-Site Request Forgery (CSRF) vulnerability in Alain Gonzalez WP RSS Images plugin <= 1.1 versions.	4.3	More Details
CVE-2023-25443	Cross-Site Request Forgery (CSRF) vulnerability in Wow-Company Button Generator – easily Button Builder plugin <= 2.3.5 versions.	4.3	More Details
CVE-2023-34185	Cross-Site Request Forgery (CSRF) vulnerability in John Brien WordPress NextGen GalleryView plugin <= 0.5.5 versions.	4.3	More Details
CVE-2023-24417	Cross-Site Request Forgery (CSRF) vulnerability in tiggersWelt.Net Worthy plugin <= 1.6.5-6497609 versions.	4.3	More Details
CVE-2023-35047	Cross-Site Request Forgery (CSRF) vulnerability in AREOI All Bootstrap Blocks plugin <= 1.3.6 versions.	4.3	More Details
CVE-2023-23546	A misconfiguration vulnerability exists in the urvpn_client functionality of Milesight UR32L v32.3.0.5. A specially-crafted man-in-the-middle attack can lead to increased privileges. An attacker can perform a man-in-the-middle attack to trigger this vulnerability.	4.2	More Details
CVE-2023-28001	An insufficient session expiration in Fortinet FortiOS 7.0.0 - 7.0.12 and 7.2.0 - 7.2.4 allows an attacker to execute unauthorized code or commands via reusing the session of a deleted user in the REST API.	4.1	More Details

CVE Number	Description	Base Score	Reference
CVE-2022-29562	A vulnerability has been identified in RUGGEDCOM ROX MX5000 (All versions < V2.16.0), RUGGEDCOM ROX MX5000RE (All versions < V2.16.0), RUGGEDCOM ROX RX1400 (All versions < V2.16.0), RUGGEDCOM ROX RX1500 (All versions < V2.16.0), RUGGEDCOM ROX RX1501 (All versions < V2.16.0), RUGGEDCOM ROX RX1510 (All versions < V2.16.0), RUGGEDCOM ROX RX1511 (All versions < V2.16.0), RUGGEDCOM ROX RX1512 (All versions < V2.16.0), RUGGEDCOM ROX RX1524 (All versions < V2.16.0), RUGGEDCOM ROX RX1536 (All versions < V2.16.0), RUGGEDCOM ROX RX5000 (All versions < V2.16.0). Affected devices do not properly handle malformed HTTP packets. This could allow an unauthenticated remote attacker to send a malformed HTTP packet causing certain functions to fail in a controlled manner.	3.7	More Details
CVE-2023-37264	Tekton Pipelines project provides k8s-style resources for declaring CI/CD-style pipelines. Starting in version 0.35.0, pipelines do not validate child UIDs, which means that a user that has access to create TaskRuns can create their own Tasks that the Pipelines controller will accept as the child Task. While the software stores and validates the PipelineRun's (api version, kind, name, uid) in the child Run's OwnerReference, it only store (api version, kind, name) in the ChildStatusReference. This means that if a client had access to create TaskRuns on a cluster, they could create a child TaskRun for a pipeline with the same name + owner reference, and the Pipeline controller picks it up as if it was the original TaskRun. This is problematic since it can let users modify the config of Pipelines at runtime, which violates SLSA L2 Service Generated / Non-falsifiable requirements. This issue can be used to trick the Pipeline controller into associating unrelated Runs to the Pipeline, feeding its data through the rest of the Pipeline. This requires access to create TaskRuns, so impact may vary depending on one Tekton setup. If users already have unrestricted access to create any Task/PipelineRun, this does not grant any additional capabilities. As of time of publication, there are no known patches for this issue.	3.7	More Details
CVE-2023-3539	A vulnerability, which was classified as problematic, has been found in SimplePHPscripts Simple Forum PHP 2.7. This issue affects some unknown processing of the file /preview.php of the component URL Parameter Handler. The manipulation leads to cross site scripting. The attack may be initiated remotely. The associated identifier of this vulnerability is VDB-233291.	3.5	More Details

CVE Number	Description	Base Score	Reference
CVE-2015-10120	A vulnerability, which was classified as problematic, was found in WDS Multisite Aggregate Plugin up to 1.0.0 on WordPress. Affected is the function update_options of the file includes/WDS_Multisite_Aggregate_Options.php. The manipulation leads to cross site scripting. It is possible to launch the attack remotely. Upgrading to version 1.0.1 is able to address this issue. The name of the patch is 49e0bbcb6ff70e561365d9e0d26426598f63ca12. It is recommended to upgrade the affected component. The identifier of this vulnerability is VDB-233364.	3.5	More Details
CVE-2015-10121	A vulnerability has been found in Beeliked Microsite Plugin up to 1.0.1 on WordPress and classified as problematic. Affected by this vulnerability is the function embed_handler of the file beelikedmicrosite.php. The manipulation leads to cross site scripting. The attack can be launched remotely. Upgrading to version 1.0.2 is able to address this issue. The identifier of the patch is d23bafb5d05fb2636a2b78331f9d3fca152903dc. It is recommended to upgrade the affected component. The identifier VDB-233365 was assigned to this vulnerability.	3.5	More Details
CVE-2015-10119	A vulnerability, which was classified as problematic, has been found in View All Posts Page Plugin up to 0.9.0 on WordPress. This issue affects the function action_admin_notices_activation of the file view-all-posts-pages.php. The manipulation leads to cross site scripting. The attack may be initiated remotely. Upgrading to version 0.9.1 is able to address this issue. The patch is named bf914f3a59063fa4df8fd4925ae18a5d852396d7. It is recommended to upgrade the affected component. The associated identifier of this vulnerability is VDB-233363.	3.5	More Details
CVE-2023-3544	A vulnerability was found in GZ Scripts Time Slot Booking Calendar PHP 1.8. It has been declared as problematic. This vulnerability affects unknown code of the file /load.php. The manipulation of the argument first_name/second_name/phone/address_1/country leads to cross site scripting. The attack can be initiated remotely. The identifier of this vulnerability is VDB-233296. NOTE: The vendor was contacted early about this disclosure but did not respond in any way.	3.5	More Details
CVE-2023-3543	A vulnerability was found in GZ Scripts Availability Booking Calendar PHP 1.8. It has been classified as problematic. This affects an unknown part of the file load.php of the component HTTP POST Request Handler. The manipulation of the argument cid/first_name/second_name/address_1/country leads to cross site scripting. It is possible to initiate the attack remotely. The associated identifier of this vulnerability is VDB-233295. NOTE: The vendor was contacted early about this disclosure but did not respond in any way.	3.5	More Details

CVE Number	Description	Base Score	Reference
CVE-2023-3535	A vulnerability was found in SimplePHPscripts FAQ Script PHP 2.3. It has been declared as problematic. Affected by this vulnerability is an unknown functionality of the file /preview.php of the component URL Parameter Handler. The manipulation leads to cross site scripting. The attack can be launched remotely. The associated identifier of this vulnerability is VDB-233287.	3.5	More Details
CVE-2023-3542	A vulnerability was found in ThinuTech ThinuCMS 1.5 and classified as problematic. Affected by this issue is some unknown functionality of the file /contact.php. The manipulation of the argument name/body leads to cross site scripting. The attack may be launched remotely. VDB-233294 is the identifier assigned to this vulnerability.	3.5	More Details
CVE-2023-3537	A vulnerability classified as problematic has been found in SimplePHPscripts News Script PHP Pro 2.4. This affects an unknown part of the file /preview.php of the component URL Parameter Handler. The manipulation leads to cross site scripting. It is possible to initiate the attack remotely. The identifier VDB-233289 was assigned to this vulnerability.	3.5	More Details
CVE-2023-3541	A vulnerability has been found in ThinuTech ThinuCMS 1.5 and classified as problematic. Affected by this vulnerability is an unknown functionality of the file /author_posts.php. The manipulation of the argument author with the input g6g12<script>alert(1)</script>o8sdm leads to cross site scripting. The attack can be launched remotely. The identifier VDB-233293 was assigned to this vulnerability.	3.5	More Details
CVE-2023-3536	A vulnerability was found in SimplePHPscripts Funeral Script PHP 3.1. It has been rated as problematic. Affected by this issue is some unknown functionality of the file /preview.php of the component URL Parameter Handler. The manipulation leads to cross site scripting. The attack may be launched remotely. The identifier of this vulnerability is VDB-233288.	3.5	More Details
CVE-2023-3540	A vulnerability, which was classified as problematic, was found in SimplePHPscripts NewsLetter Script PHP 2.4. Affected is an unknown function of the file /preview.php of the component URL Parameter Handler. The manipulation leads to cross site scripting. It is possible to launch the attack remotely. The identifier of this vulnerability is VDB-233292.	3.5	More Details
CVE-2023-3538	A vulnerability classified as problematic was found in SimplePHPscripts Photo Gallery PHP 2.0. This vulnerability affects unknown code of the file /preview.php of the component URL Parameter Handler. The manipulation leads to cross site scripting. The attack can be initiated remotely. VDB-233290 is the identifier assigned to this vulnerability.	3.5	More Details

CVE Number	Description	Base Score	Reference
CVE-2023-3560	A vulnerability, which was classified as problematic, has been found in GZ Scripts Ticket Booking Script 1.8. Affected by this issue is some unknown functionality of the file /load.php. The manipulation of the argument first_name/second_name/phone/address_1/country leads to cross site scripting. The attack may be launched remotely. VDB-233354 is the identifier assigned to this vulnerability. NOTE: The vendor was contacted early about this disclosure but did not respond in any way.	3.5	More Details
CVE-2023-3558	A vulnerability classified as problematic has been found in GZ Scripts Event Booking Calendar 1.8. Affected is an unknown function of the file /load.php. The manipulation of the argument first_name/second_name/phone/address_1/country leads to cross site scripting. It is possible to launch the attack remotely. The identifier of this vulnerability is VDB-233352. NOTE: The vendor was contacted early about this disclosure but did not respond in any way.	3.5	More Details
CVE-2023-3559	A vulnerability classified as problematic was found in GZ Scripts PHP GZ Appointment Scheduling Script 1.8. Affected by this vulnerability is an unknown functionality of the file /load.php. The manipulation of the argument first_name/second_name/phone/address_1/country leads to cross site scripting. The attack can be launched remotely. The identifier VDB-233353 was assigned to this vulnerability. NOTE: The vendor was contacted early about this disclosure but did not respond in any way.	3.5	More Details
CVE-2023-1936	An issue has been discovered in GitLab CE/EE affecting all versions starting from 13.7 before 15.11.10, all versions starting from 16.0 before 16.0.6, all versions starting from 16.1 before 16.1.1, which allows an attacker to leak the email address of a user who created a service desk issue.	3.5	More Details
CVE-2023-3566	A vulnerability was found in wallabag 2.5.4. It has been declared as problematic. Affected by this vulnerability is an unknown functionality of the file /config of the component Profile Config. The manipulation of the argument Name leads to allocation of resources. The exploit has been disclosed to the public and may be used. The associated identifier of this vulnerability is VDB-233359. NOTE: The vendor was contacted early about this disclosure but did not respond in any way.	3.5	More Details
CVE-2023-3564	A vulnerability was found in GZ Scripts GZ Multi Hotel Booking System 1.8. It has been classified as problematic. Affected is an unknown function of the file /index.php. The manipulation of the argument adults/children/cal_id leads to cross site scripting. It is possible to launch the attack remotely. VDB-233358 is the identifier assigned to this vulnerability.	3.5	More Details

CVE Number	Description	Base Score	Reference
CVE-2023-3209	The MStore API WordPress plugin before 3.9.7 does not secure most of its AJAX actions by implementing privilege checks, nonce checks, or a combination of both.	3.5	More Details
CVE-2023-3554	A vulnerability was found in GZ Scripts GZ Forum Script 1.8 and classified as problematic. Affected by this issue is some unknown functionality of the file /preview.php. The manipulation of the argument catid/topicid/topic/topic_message/free_name leads to cross site scripting. The attack may be launched remotely. The identifier of this vulnerability is VDB-233348. NOTE: The vendor was contacted early about this disclosure but did not respond in any way.	3.5	More Details
CVE-2023-3563	A vulnerability was found in GZ Scripts GZ E Learning Platform 1.8 and classified as problematic. This issue affects some unknown processing of the component URL Parameter Handler. The manipulation leads to cross site scripting. The attack may be initiated remotely. The identifier VDB-233357 was assigned to this vulnerability.	3.5	More Details
CVE-2023-3555	A vulnerability was found in GZ Scripts PHP Vacation Rental Script 1.8. It has been classified as problematic. This affects an unknown part of the file /preview.php. The manipulation of the argument page/layout/sort_by/property_id leads to cross site scripting. It is possible to initiate the attack remotely. The identifier VDB-233349 was assigned to this vulnerability. NOTE: The vendor was contacted early about this disclosure but did not respond in any way.	3.5	More Details
CVE-2023-3556	A vulnerability was found in GZ Scripts Car Listing Script PHP 1.8. It has been declared as problematic. This vulnerability affects unknown code of the file /preview.php. The manipulation of the argument page/sort_by leads to cross site scripting. The attack can be initiated remotely. VDB-233350 is the identifier assigned to this vulnerability. NOTE: The vendor was contacted early about this disclosure but did not respond in any way.	3.5	More Details
CVE-2023-3557	A vulnerability was found in GZ Scripts Property Listing Script 1.0. It has been rated as problematic. This issue affects some unknown processing of the file /preview.php. The manipulation of the argument page/layout/sort_by leads to cross site scripting. The attack may be initiated remotely. The associated identifier of this vulnerability is VDB-233351. NOTE: The vendor was contacted early about this disclosure but did not respond in any way.	3.5	More Details

CVE Number	Description	Base Score	Reference
CVE-2023-3562	A vulnerability has been found in GZ Scripts PHP CRM Platform 1.8 and classified as problematic. This vulnerability affects unknown code of the file /index.php. The manipulation of the argument action leads to cross site scripting. The attack can be initiated remotely. The identifier of this vulnerability is VDB-233356. NOTE: The vendor was contacted early about this disclosure but did not respond in any way.	3.5	More Details
CVE-2023-3561	A vulnerability, which was classified as problematic, was found in GZ Scripts PHP GZ Hotel Booking Script 1.8. This affects an unknown part of the file /load.php. The manipulation of the argument first_name/second_name/phone/address_1/country leads to cross site scripting. It is possible to initiate the attack remotely. The associated identifier of this vulnerability is VDB-233355. NOTE: The vendor was contacted early about this disclosure but did not respond in any way.	3.5	More Details
CVE-2023-34117	Relative path traversal in the Zoom Client SDK before version 5.15.0 may allow an unauthorized user to enable information disclosure via local access.	3.3	More Details
CVE-2023-30648	Stack out-of-bounds write vulnerability in IpcRxImeiUpdateImeiNoti of RILD priro to SMR Jul-2023 Release 1 cause a denial of service on the system.	3.3	More Details
CVE-2023-34442	Exposure of Sensitive Information to an Unauthorized Actor vulnerability in Apache Software Foundation Apache Camel.This issue affects Apache Camel: from 3.X through <=3.14.8, from 3.18.X through <=3.18.7, from 3.20.X through <= 3.20.5, from 4.X through <= 4.0.0-M3. Users should upgrade to 3.14.9, 3.18.8, 3.20.6 or 3.21.0 and for users on Camel 4.x update to 4.0.0-M1	3.3	More Details
CVE-2023-28953	IBM Cognos Analytics on Cloud Pak for Data 4.0 could allow an attacker to make system calls that might compromise the security of the containers due to misconfigured security context. IBM X-Force ID: 251465.	3.1	More Details

CVE Number	Description	Base Score	Reference
CVE-2023-37269	Winter is a free, open-source content management system (CMS) based on the Laravel PHP framework. Users with the `backend.manage_branding` permission can upload SVGs as the application logo. Prior to version 1.2.3, SVG uploads were not sanitized, which could have allowed a stored cross-site scripting (XSS) attack. To exploit the vulnerability, an attacker would already need to have developer or super user level permissions in Winter CMS. This means they would already have extensive access and control within the system. Additionally, to execute the XSS, the attacker would need to convince the victim to directly visit the URL of the maliciously uploaded SVG, and the application would have to be using local storage where uploaded files are served under the same domain as the application itself instead of a CDN. This is because all SVGs in Winter CMS are rendered through an `img` tag, which prevents any payloads from being executed directly. These two factors significantly limit the potential harm of this vulnerability. This issue has been patched in v1.2.3 through the inclusion of full support for SVG uploads and automatic sanitization of uploaded SVG files. As a workaround, one may apply the patches manually.	2.0	More Details
CVE-2023-33715	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-2023-37151	Rejected reason: DO NOT USE THIS CANDIDATE NUMBER. ConsultIDs: CVE-2023-2246. Reason: This candidate is a reservation duplicate of CVE-2023-2246. Notes: All CVE users should reference CVE-2023-2246 instead of this candidate. All references and descriptions in this candidate have been removed to prevent accidental usage.	N/A	More Details
CVE-2023-36935	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-2023-36360	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-2023-36164	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-2023-36167	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-2023-34682	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