SingCERT
Singapore Cyber Emergency Response Team

Security Bulletin 02 August 2023

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

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

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

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

CRITICAL VULNERABILITIES

CVE Number	Description	Base Score	Reference
CVE-2023-38647	An attacker can use SnakeYAML to deserialize java.net.URLClassLoader and make it load a JAR from a specified URL, and then deserialize javax.script.ScriptEngineManager to load code using that ClassLoader. This unbounded deserialization can likely lead to remote code execution. The code can be run in Helix REST start and Workflow creation. Affect all the versions lower and include 1.2.0. Affected products: helix-core, helix-rest Mitigation: Short term, stop using any YAML based configuration and workflow creation. Long term, all Helix version bumping up to 1.3.0	9.8	More Details
CVE-2023-36091	Authentication Bypass vulnerability in D-Link DIR-895 FW102b07 allows remote attackers to gain escalated privileges via via function phpcgi_main in cgibin. NOTE: This vulnerability only affects products that are no longer supported by the maintainer.	9.8	More Details

CVE Number	Description	Base Score	Reference
CVE-2023-37214	Heights Telecom ERO1xS-Pro Dual-Band FW version BZ_ERO1XP.025.	9.8	More Details
CVE-2023-4005	Insufficient Session Expiration in GitHub repository fossbilling/fossbilling prior to 0.5.5.	9.8	More Details
CVE-2023-4006	Improper Neutralization of Formula Elements in a CSV File in GitHub repository thorsten/phpmyfaq prior to 3.1.16.	9.8	More Details
CVE-2023-35861	A shell-injection vulnerability in email notifications on Supermicro motherboards (such as H12DST-B before 03.10.35) allows remote attackers to inject execute arbitrary commands as root on the BMC.	9.8	More Details
CVE-2023-37647	SEMCMS v1.5 was discovered to contain a SQL injection vulnerability via the id parameter at /Ant_Suxin.php.	9.8	More Details
CVE-2020-21662	SQL injection vulnerability in yunyecms 2.0.2 allows remote attackers to run arbitrary SQL commands via XFF.	9.8	More Details
CVE-2023-34635	Wifi Soft Unibox Administration 3.0 and 3.1 is vulnerable to SQL Injection. The vulnerability occurs because of not validating or sanitizing the user input in the username field of the login page.	9.8	More Details
CVE-2023-34644	Remote code execution vulnerability in Ruijie Networks Product: RG-EW series home routers and repeaters EW_3.0(1)B11P204, RG-NBS and RG-S1930 series switches SWITCH_3.0(1)B11P218, RG-EG series business VPN routers EG_3.0(1)B11P216, EAP and RAP series wireless access points AP_3.0(1)B11P218, NBC series wireless controllers AC_3.0(1)B11P86 allows unauthorized remote attackers to gain the highest privileges via crafted POST request to /cgi-bin/luci/api/auth.	9.8	More Details
CVE-2023-34842	Remote Code Execution vulnerability in DedeCMS through 5.7.109 allows remote attackers to run arbitrary code via crafted POST request to /dede/tpl.php.	9.8	More Details
CVE-2023-36089	Authentication Bypass vulnerability in D-Link DIR-645 firmware version 1.03 allows remote attackers to gain escalated privileges via function phpcgi_main in cgibin. NOTE: This vulnerability only affects products that are no longer supported by the maintainer.	9.8	More Details

CVE Number	Description	Base Score	Reference
CVE-2023-36090	Authentication Bypass vulnerability in D-Link DIR-885L FW102b01 allows remote attackers to gain escalated privileges via phpcgi. NOTE: This vulnerability only affects products that are no longer supported by the maintainer.	9.8	More Details
CVE-2023-36092	Authentication Bypass vulnerability in D-Link DIR-859 FW105b03 allows remote attackers to gain escalated privileges via via phpcgi_main. NOTE: This vulnerability only affects products that are no longer supported by the maintainer.	9.8	More Details
CVE-2023-32225	Sysaid - CWE-434: Unrestricted Upload of File with Dangerous Type - A malicious user with administrative privileges may be able to upload a dangerous filetype via an unspecified method.	9.8	More Details
CVE-2023-37771	Art Gallery Management System v1.0 contains a SQL injection vulnerability via the cid parameter at /agms/product.php.	9.8	More Details
CVE-2023-39122	BMC Control-M through 9.0.20.200 allows SQL injection via the /RF-Server/report/deleteReport report-id parameter. This is fixed in 9.0.21 (and is also fixed by a patch for 9.0.20.200).	9.8	More Details
CVE-2023-34960	A command injection vulnerability in the wsConvertPpt component of Chamilo v1.11.* up to v1.11.18 allows attackers to execute arbitrary commands via a SOAP API call with a crafted PowerPoint name.	9.8	More Details
CVE-2022-39986	A Command injection vulnerability in RaspAP 2.8.0 thru 2.8.7 allows unauthenticated attackers to execute arbitrary commands via the cfg_id parameter in /ajax/openvpn/activate_ovpncfg.php and /ajax/openvpn/del_ovpncfg.php.	9.8	More Details
CVE-2023-31710	TP-Link Archer AX21(US)_V3_1.1.4 Build 20230219 and AX21(US)_V3.6_1.1.4 Build 20230219 are vulnerable to Buffer Overflow.	9.8	More Details
CVE-2023-4056	Memory safety bugs present in Firefox 115, Firefox ESR 115.0, Firefox ESR 102.13, Thunderbird 115.0, and Thunderbird 102.13. 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 < 116, Firefox ESR < 102.14, and Firefox ESR < 115.1.	9.8	More Details

CVE Number	Description	Base Score	Reference
CVE-2023-4057	Memory safety bugs present in Firefox 115, Firefox ESR 115.0, and Thunderbird 115.0. 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 < 116, Firefox ESR < 115.1, and Thunderbird < 115.1.	9.8	More Details
CVE-2023-4058	Memory safety bugs present in Firefox 115. 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 < 116.	9.8	More Details
CVE-2023-33493	An Unrestricted Upload of File with Dangerous Type vulnerability in the Ajaxmanager File and Database explorer (ajaxmanager) module for PrestaShop through 2.3.0, allows remote attackers to upload dangerous files without restrictions.	9.8	More Details
CVE-2023-36210	MotoCMS Version 3.4.3 Store Category Template was discovered to contain a Server-Side Template Injection (SSTI) vulnerability via the keyword parameter.	9.8	More Details
CVE-2023-33561	Improper input validation of password parameter in PHP Jabbers Time Slots Booking Calendar v 3.3 results in insecure passwords.	9.8	More Details
CVE-2023-32227	Synel SYnergy Fingerprint Terminals - CWE-798: Use of Hard-coded Credentials	9.8	More Details
CVE-2023-33562	User enumeration is found in in PHP Jabbers Time Slots Booking Calendar v3.3. This issue occurs during password recovery, where a difference in messages could allow an attacker to determine if the user is valid or not, enabling a brute force attack with valid users.	9.8	More Details
CVE-2023-38598	A use-after-free issue was addressed with improved memory management. This issue is fixed in watchOS 9.6, macOS Big Sur 11.7.9, iOS 15.7.8 and iPadOS 15.7.8, macOS Monterey 12.6.8, tvOS 16.6, iOS 16.6 and iPadOS 16.6, macOS Ventura 13.5. An app may be able to execute arbitrary code with kernel privileges.	9.8	More Details
CVE-2023-31465	An issue was discovered in FSMLabs TimeKeeper 8.0.17 through 8.0.28. By intercepting requests from various timekeeper streams, it is possible to find the getsamplebacklog call. Some query parameters are passed directly in the URL and named arg[x], with x an integer starting from 1; it is possible to modify arg[2] to insert Bash code that will be executed directly by the server.	9.8	More Details

CVE Number	Description	Base Score	Reference
CVE-2023-3974	OS Command Injection in GitHub repository jgraph/drawio prior to 21.4.0.	9.8	More Details
CVE-2023-3975	OS Command Injection in GitHub repository jgraph/drawio prior to 21.5.0.	9.8	More Details
CVE-2023-33743	TeleAdapt RoomCast TA-2400 1.0 through 3.1 is vulnerable to Improper Access Control; specifically, Android Debug Bridge (adb) is available.	9.8	More Details
CVE-2023-33744	TeleAdapt RoomCast TA-2400 1.0 through 3.1 suffers from Use of a Hard-coded Password (PIN): 385521, 843646, and 592671.	9.8	More Details
CVE-2023-33745	TeleAdapt RoomCast TA-2400 1.0 through 3.1 is vulnerable to Improper Privilege Management: from the shell available after an adb connection, simply entering the su command provides root access (without requiring a password).	9.8	More Details
CVE-2023-34425	The issue was addressed with improved memory handling. This issue is fixed in watchOS 9.6, macOS Monterey 12.6.8, iOS 15.7.8 and iPadOS 15.7.8, macOS Big Sur 11.7.9, iOS 16.6 and iPadOS 16.6, macOS Ventura 13.5. An app may be able to execute arbitrary code with kernel privileges.	9.8	More Details
CVE-2023-33308	A stack-based overflow vulnerability [CWE-124] in Fortinet FortiOS version 7.0.0 through 7.0.10 and 7.2.0 through 7.2.3 and FortiProxy version 7.0.0 through 7.0.9 and 7.2.0 through 7.2.2 allows a remote unauthenticated attacker to execute arbitrary code or command via crafted packets reaching proxy policies or firewall policies with proxy mode alongside deep or full packet inspection.	9.8	More Details
CVE-2023-36495	An integer overflow was addressed with improved input validation. This issue is fixed in watchOS 9.6, macOS Monterey 12.6.8, iOS 15.7.8 and iPadOS 15.7.8, tvOS 16.6, iOS 16.6 and iPadOS 16.6, macOS Ventura 13.5. An app may be able to execute arbitrary code with kernel privileges.	9.8	More Details
CVE-2023-37285	An out-of-bounds read was addressed with improved bounds checking. This issue is fixed in iOS 15.7.8 and iPadOS 15.7.8, macOS Big Sur 11.7.9, macOS Monterey 12.6.8, macOS Ventura 13.5. An app may be able to execute arbitrary code with kernel privileges.	9.8	More Details

CVE Number	Description	Base Score	Reference
CVE-2023-26859	SQL injection vulnerability found in PrestaShop sendinblue v.4.0.15 and before allow a remote attacker to gain privileges via the ajaxOrderTracking.php component.	9.8	More Details
CVE-2023-38604	An out-of-bounds write issue was addressed with improved input validation. This issue is fixed in watchOS 9.6, macOS Big Sur 11.7.9, iOS 15.7.8 and iPadOS 15.7.8, macOS Monterey 12.6.8, tvOS 16.6, iOS 16.6 and iPadOS 16.6, macOS Ventura 13.5. An app may be able to execute arbitrary code with kernel privileges.	9.8	More Details
CVE-2023-37754	PowerJob v4.3.3 was discovered to contain a remote command execution (RCE) vulnerability via the instanceId parameter at /instance/detail.	9.8	More Details
CVE-2023-38992	jeecg-boot v3.5.1 was discovered to contain a SQL injection vulnerability via the title parameter at /sys/dict/loadTreeData.	9.8	More Details
CVE-2023-39010	BoofCV 0.42 was discovered to contain a code injection vulnerability via the component boofcv.io.calibration.CalibrationIO.load. This vulnerability is exploited by loading a crafted camera calibration file.	9.8	More Details
CVE-2023-39013	Duke v1.2 and below was discovered to contain a code injection vulnerability via the component no.priv.garshol.duke.server.CommonJTimer.init.	9.8	More Details
CVE-2023-39015	webmagic-extension v0.9.0 and below was discovered to contain a code injection vulnerability via the component us.codecraft.webmagic.downloader.PhantomJSDownloader.	9.8	More Details
CVE-2023-39016	bboss-persistent v6.0.9 and below was discovered to contain a code injection vulnerability in the component com.frameworkset.common.poolman.util.SQLManager.createPool. This vulnerability is exploited via passing an unchecked argument.	9.8	More Details
CVE-2023-39017	quartz-jobs 2.3.2 and below was discovered to contain a code injection vulnerability in the component org.quartz.jobs.ee.jms.SendQueueMessageJob.execute. This vulnerability is exploited via passing an unchecked argument. NOTE: this is disputed by multiple parties because it is not plausible that untrusted user input would reach the code location where injection must occur.	9.8	More Details

CVE Number	Description	Base Score	Reference
CVE-2023-39018	FFmpeg 0.7.0 and below was discovered to contain a code injection vulnerability in the component net.bramp.ffmpeg.FFmpeg.<constructor>. This vulnerability is exploited via passing an unchecked argument. NOTE: this is disputed by multiple third parties because there are no realistic use cases in which FFmpeg.java uses untrusted input for the path of the executable file.	9.8	More Details
CVE-2023-39020	stanford-parser v3.9.2 and below was discovered to contain a code injection vulnerability in the component edu.stanford.nlp.io.getBZip2PipedInputStream. This vulnerability is exploited via passing an unchecked argument.	9.8	More Details
CVE-2023-39021	wix-embedded-mysql v4.6.1 and below was discovered to contain a code injection vulnerability in the component com.wix.mysql.distribution.Setup.apply. This vulnerability is exploited via passing an unchecked argument.	9.8	More Details
CVE-2023-39022	oscore v2.2.6 and below was discovered to contain a code injection vulnerability in the component com.opensymphony.util.EJBUtils.createStateless. This vulnerability is exploited via passing an unchecked argument.	9.8	More Details
CVE-2023-39023	university compass v2.2.0 and below was discovered to contain a code injection vulnerability in the component org.compass.core.executor.DefaultExecutorManager.configure. This vulnerability is exploited via passing an unchecked argument.	9.8	More Details
CVE-2023-3956	The InstaWP Connect plugin for WordPress is vulnerable to unauthorized access of data, modification of data and loss of data due to a missing capability check on the 'events_receiver' function in versions up to, and including, 0.0.9.18. This makes it possible for unauthenticated attackers to add, modify or delete post and taxonomy, install, activate or deactivate plugin, change customizer settings, add or modify or delete user including administrator user.	9.8	More Details
CVE-2022-4920	Heap buffer overflow in Blink in Google Chrome prior to 101.0.4951.41 allowed a remote attacker who convinced a user to engage in specific UI gestures to potentially perform a sandbox escape via a crafted HTML page. (Chromium security severity: High)	9.6	More Details
CVE-2023-38673	PaddlePaddle before 2.5.0 has a command injection in fs.py. This resulted in the ability to execute arbitrary commands on the operating system.	9.6	More Details

CVE Number	Description	Base Score	Reference
CVE-2022-4924	Use after free in WebRTC in Google Chrome prior to 97.0.4692.71 allowed a remote attacker who had compromised the renderer process to potentially perform a sandbox escape via a crafted HTML page. (Chromium security severity: High)	9.6	More Details
CVE-2022-42183	Precisely Spectrum Spatial Analyst 20.01 is vulnerable to Server-Side Request Forgery (SSRF).	9.1	More Details

OTHER VULNERABILITIES

CVE Number	Description	Base Score	Reference
CVE-2023-3728	Use after free in WebRTC in Google Chrome prior to 115.0.5790.98 allowed a remote attacker to potentially exploit heap corruption via a crafted HTML page. (Chromium security severity: High)	8.8	More Details
CVE-2023-38611	The issue was addressed with improved memory handling. This issue is fixed in iOS 16.6 and iPadOS 16.6, tvOS 16.6, macOS Ventura 13.5, Safari 16.6, watchOS 9.6. Processing web content may lead to arbitrary code execution.	8.8	More Details
CVE-2023-3598	Out of bounds read and write in ANGLE in Google Chrome prior to 114.0.5735.90 allowed a remote attacker to potentially exploit heap corruption via a crafted HTML page. (Chromium security severity: High)	8.8	More Details
CVE-2023-38600	The issue was addressed with improved checks. This issue is fixed in iOS 16.6 and iPadOS 16.6, tvOS 16.6, macOS Ventura 13.5, Safari 16.6, watchOS 9.6. Processing web content may lead to arbitrary code execution.	8.8	More Details
CVE-2021-4322	Use after free in DevTools in Google Chrome prior to 91.0.4472.77 allowed an attacker who convinced a user to install a malicious extension to execute arbitrary code via a crafted Chrome Extension. (Chromium security severity: Medium)	8.8	More Details
CVE-2023-38595	The issue was addressed with improved checks. This issue is fixed in iOS 16.6 and iPadOS 16.6, tvOS 16.6, macOS Ventura 13.5, Safari 16.6, watchOS 9.6. Processing web content may lead to arbitrary code execution.	8.8	More Details

CVE Number	Description	Base Score	Reference
CVE-2023-3718	An authenticated command injection vulnerability exists in the AOS-CX command line interface. Successful exploitation of this vulnerability results in the ability to execute arbitrary commands on the underlying operating system as a privileged user on the affected switch. This allows an attacker to fully compromise the underlying operating system on the device running AOS-CX.	8.8	More Details
CVE-2023-33563	In PHP Jabbers Time Slots Booking Calendar 3.3 , lack of verification when changing an email address and/or password (on the Profile Page) allows remote attackers to take over accounts.	8.8	More Details
CVE-2022-4906	Inappropriate implementation in Blink in Google Chrome prior to 108.0.5359.71 allowed a remote attacker to perform arbitrary read/write via a crafted HTML page. (Chromium security severity: High)	8.8	More Details
CVE-2023-3730	Use after free in Tab Groups in Google Chrome prior to 115.0.5790.98 allowed a remote attacker who convinced a user to engage in specific UI interactions to potentially exploit heap corruption via a crafted HTML page. (Chromium security severity: High)	8.8	More Details
CVE-2023-3729	Use after free in Splitscreen in Google Chrome on ChromeOS prior to 115.0.5790.131 allowed a remote attacker who convinced a user to engage in specific UI interactions to potentially exploit heap corruption via crafted UI interactions. (Chromium security severity: High)	8.8	More Details
CVE-2023-34552	In certain EZVIZ products, two stack based buffer overflows in mulicast_parse_sadp_packet and mulicast_get_pack_type functions of the SADP multicast protocol can allow an unauthenticated attacker present on the same local network as the camera to achieve remote code execution. This affects CS-C6N-B0-1G2WF Firmware versions before V5.3.0 build 230215 and CS-C6N-R101-1G2WF Firmware versions before V5.3.0 build 230215 and CS-CV310-A0-1B2WFR Firmware versions before V5.3.0 build 230221 and CS-CV310-A0-1C2WFR-C Firmware versions before V5.3.2 build 230221 and CS-C6N-A0-1C2WFR-MUL Firmware versions before V5.3.2 build 230218 and CS-CV310-A0-3C2WFRL-1080p Firmware versions before V5.2.7 build 230302 and CS-CV310-A0-1C2WFR Wifi IP66 2.8mm 1080p Firmware versions before V5.3.2 build 230214 and CS-CV248-A0-32WMFR Firmware versions before V5.2.3 build 230217 and EZVIZ LC1C Firmware versions before V5.3.4 build 230214.	8.8	More Details
CVE-2022-4907	Uninitialized Use in FFmpeg in Google Chrome prior to 108.0.5359.71 allowed a remote attacker to execute arbitrary code inside a sandbox via a crafted HTML page. (Chromium security severity: Medium)	8.8	More Details

CVE Number	Description	Base Score	Reference
CVE-2023-37213	Synel SYnergy Fingerprint Terminals - CWE-78: 'OS Command Injection'	8.8	More Details
CVE-2022-4912	Type Confusion in MathML in Google Chrome prior to 105.0.5195.52 allowed a remote attacker to potentially exploit heap corruption via a crafted HTML page. (Chromium security severity: High)	8.8	More Details
CVE-2022-4914	Heap buffer overflow in PrintPreview in Google Chrome prior to 104.0.5112.79 allowed an attacker who convinced a user to install a malicious extension to potentially exploit heap corruption via a crafted HTML page. (Chromium security severity: Medium)	8.8	More Details
CVE-2023-36542	Apache NiFi 0.0.2 through 1.22.0 include Processors and Controller Services that support HTTP URL references for retrieving drivers, which allows an authenticated and authorized user to configure a location that enables custom code execution. The resolution introduces a new Required Permission for referencing remote resources, restricting configuration of these components to privileged users. The permission prevents unprivileged users from configuring Processors and Controller Services annotated with the new Reference Remote Resources restriction. Upgrading to Apache NiFi 1.23.0 is the recommended mitigation.	8.8	More Details
CVE-2023-2313	Inappropriate implementation in Sandbox in Google Chrome on Windows prior to 112.0.5615.49 allowed a remote attacker who had compromised the renderer process to perform arbitrary read/write via a malicious file. (Chromium security severity: High)	8.8	More Details
CVE-2023-3727	Use after free in WebRTC in Google Chrome prior to 115.0.5790.98 allowed a remote attacker to potentially exploit heap corruption via a crafted HTML page. (Chromium security severity: High)	8.8	More Details
CVE-2023-4047	A bug in popup notifications delay calculation could have made it possible for an attacker to trick a user into granting permissions. This vulnerability affects Firefox < 116, Firefox ESR < 102.14, and Firefox ESR < 115.1.	8.8	More Details
CVE-2022-4921	Use after free in Accessibility in Google Chrome prior to 99.0.4844.51 allowed a remote attacker who convinced a user to engage in specific UI gestures to perform arbitrary read/write via a crafted HTML page. (Chromium security severity: Low)	8.8	More Details
CVE-2022-4919	Use after free in Base Internals in Google Chrome prior to 101.0.4951.41 allowed a remote attacker to perform arbitrary read/write via a crafted HTML page. (Chromium security severity: High)	8.8	More Details

CVE Number	Description	Base Score	Reference
CVE-2023-3494	The fwctl driver implements a state machine which is executed when a bhyve guest accesses certain x86 I/O ports. The interface lets the guest copy a string into a buffer resident in the bhyve process' memory. A bug in the state machine implementation can result in a buffer overflowing when copying this string. Malicious, privileged software running in a guest VM can exploit the buffer overflow to achieve code execution on the host in the bhyve userspace process, which typically runs as root, mitigated by the capabilities assigned through the Capsicum sandbox available to the bhyve process.	8.8	More Details
CVE-2022-4916	Use after free in Media in Google Chrome prior to 103.0.5060.53 allowed a remote attacker to perform arbitrary read/write via a crafted HTML page. (Chromium security severity: High)	8.8	More Details
CVE-2023-33534	A Cross-Site Request Forgery (CSRF) in Guanzhou Tozed Kangwei Intelligent Technology ZLTS10G software version S10G_3.11.6 allows attackers to takeover user accounts via sending a crafted POST request to /goform/goform_set_cmd_process.	8.8	More Details
CVE-2023-38592	A logic issue was addressed with improved restrictions. This issue is fixed in iOS 16.6 and iPadOS 16.6, watchOS 9.6, tvOS 16.6, macOS Ventura 13.5. Processing web content may lead to arbitrary code execution.	8.8	More Details
CVE-2023-3732	Out of bounds memory access in Mojo in Google Chrome prior to 115.0.5790.98 allowed a remote attacker who had compromised the renderer process to potentially exploit heap corruption via a crafted HTML page. (Chromium security severity: High)	8.8	More Details
CVE-2021-4317	Use after free in ANGLE in Google Chrome prior to 96.0.4664.93 allowed a remote attacker to perform arbitrary read/write via a crafted HTML page. (Chromium security severity: High)	8.8	More Details
CVE-2021-4318	Object corruption in Blink in Google Chrome prior to 94.0.4606.54 allowed a remote attacker to potentially exploit object corruption via a crafted HTML page. (Chromium security severity: High)	8.8	More Details
CVE-2023-32393	The issue was addressed with improved memory handling. This issue is fixed in watchOS 9.3, tvOS 16.3, macOS Ventura 13.2, iOS 16.3 and iPadOS 16.3. Processing web content may lead to arbitrary code execution.	8.8	More Details
CVE-2021-4319	Use after free in Blink in Google Chrome prior to 93.0.4577.82 allowed a remote attacker to perform arbitrary read/write via a crafted HTML page. (Chromium security severity: High)	8.8	More Details

CVE Number	Description	Base Score	Reference
CVE-2022-39987	A Command injection vulnerability in RaspAP 2.8.0 thru 2.9.2 allows an authenticated attacker to execute arbitrary OS commands as root via the "entity" POST parameters in /ajax/networking/get_wgkey.php.	8.8	More Details
CVE-2023-37772	Online Shopping Portal Project v3.1 was discovered to contain a SQL injection vulnerability via the Email parameter at /shopping/login.php.	8.8	More Details
CVE-2023-38597	The issue was addressed with improved checks. This issue is fixed in iOS 15.7.8 and iPadOS 15.7.8, iOS 16.6 and iPadOS 16.6, macOS Ventura 13.5, Safari 16.6. Processing web content may lead to arbitrary code execution.	8.8	More Details
CVE-2023-38555	Authentication bypass vulnerability in Fujitsu network devices Si-R series and SR-M series allows a network-adjacent unauthenticated attacker to obtain, change, and/or reset configuration settings of the affected products. Affected products and versions are as follows: Si-R 30B all versions, Si-R 130B all versions, Si-R 90brin all versions, Si-R570B all versions, Si-R370B all versions, Si-R220D all versions, Si-R G100 V02.54 and earlier, Si-R G200 V02.54 and earlier, Si-R G100B V04.12 and earlier, Si-R G110B V04.12 and earlier, Si-R G200B V04.12 and earlier, Si-R G210 V20.52 and earlier, Si-R G211 V20.52 and earlier, Si-R G120 V20.52 and earlier, Si-R G121 V20.52 and earlier, and SR-M 50AP1 all versions.	8.8	More Details
CVE-2023-38594	The issue was addressed with improved checks. This issue is fixed in iOS 15.7.8 and iPadOS 15.7.8, iOS 16.6 and iPadOS 16.6, tvOS 16.6, macOS Ventura 13.5, Safari 16.6, watchOS 9.6. Processing web content may lead to arbitrary code execution.	8.8	More Details
CVE-2023-38590	A buffer overflow issue was addressed with improved memory handling. This issue is fixed in watchOS 9.6, macOS Big Sur 11.7.9, iOS 15.7.8 and iPadOS 15.7.8, macOS Monterey 12.6.8, tvOS 16.6, iOS 16.6 and iPadOS 16.6, macOS Ventura 13.5. A remote user may be able to cause unexpected system termination or corrupt kernel memory.	8.8	More Details
CVE-2021-4320	Use after free in Blink in Google Chrome prior to 92.0.4515.107 allowed a remote attacker who had compromised the renderer process to perform arbitrary read/write via a crafted HTML page. (Chromium security severity: High)	8.8	More Details
CVE-2023-3731	Use after free in Diagnostics in Google Chrome on ChromeOS prior to 115.0.5790.131 allowed an attacker who convinced a user to install a malicious extension to potentially exploit heap corruption via a crafted Chrome Extension. (Chromium security severity: High)	8.8	More Details

CVE Number	Description	Base Score	Reference
CVE-2023-3983	An authenticated SQL injection vulnerability exists in Advantech iView versions prior to v5.7.4 build 6752. An authenticated remote attacker can bypass checks in com.imc.iview.utils.CUtils.checkSQLInjection() to perform blind SQL injection.	8.8	More Details
CVE-2023-39108	rconfig v3.9.4 was discovered to contain a Server-Side Request Forgery (SSRF) via the path_b parameter in the doDiff Function of /classes/compareClass.php. This vulnerability allows authenticated attackers to make arbitrary requests via injection of crafted URLs.	8.8	More Details
CVE-2022-43710	Interactive Forms (IAF) in GX Software XperienCentral versions 10.31.0 until 10.33.0 was vulnerable to cross site request forgery (CSRF) because the unique token could be deduced using the names of all input fields.	8.8	More Details
CVE-2023-39109	rconfig v3.9.4 was discovered to contain a Server-Side Request Forgery (SSRF) via the path_a parameter in the doDiff Function of /classes/compareClass.php. This vulnerability allows authenticated attackers to make arbitrary requests via injection of crafted URLs.	8.8	More Details
CVE-2023-39110	rconfig v3.9.4 was discovered to contain a Server-Side Request Forgery (SSRF) via the path parameter at /ajaxGetFileByPath.php. This vulnerability allows authenticated attackers to make arbitrary requests via injection of crafted URLs.	8.8	More Details
CVE-2023-37450	The issue was addressed with improved checks. This issue is fixed in iOS 16.6 and iPadOS 16.6, Safari 16.5.2, tvOS 16.6, macOS Ventura 13.5, watchOS 9.6. Processing web content may lead to arbitrary code execution. Apple is aware of a report that this issue may have been actively exploited.	8.8	More Details
CVE-2022-4918	Use after free in UI in Google Chrome prior to 102.0.5005.61 allowed a remote attacker to perform arbitrary read/write via a crafted HTML page. (Chromium security severity: Medium)	8.8	More Details
CVE-2023-3997	Splunk SOAR versions lower than 6.1.0 are indirectly affected by a potential vulnerability accessed through the user’s terminal. A third party can send Splunk SOAR a maliciously crafted web request containing special ANSI characters to cause log file poisoning. When a terminal user attempts to view the poisoned logs, this can tamper with the terminal and cause possible malicious code execution from the terminal user’s action.	8.6	More Details
CVE-2023-3242	Improper initialization implementation in Portmapper used in B&R Industrial Automation Automation Runtime <G4.93 allows unauthenticated network-based attackers to cause permanent denial-of-service conditions.	8.6	More Details

CVE Number	Description	Base Score	Reference
CVE-2023-32437	The issue was addressed with improvements to the file handling protocol. This issue is fixed in iOS 16.6 and iPadOS 16.6. An app may be able to break out of its sandbox.	8.6	More Details
CVE-2023-32364	A logic issue was addressed with improved restrictions. This issue is fixed in macOS Ventura 13.5. A sandboxed process may be able to circumvent sandbox restrictions.	8.6	More Details
CVE-2023-38495	Crossplane is a framework for building cloud native control planes without needing to write code. In versions prior to 1.11.5, 1.12.3, and 1.13.0, Crossplane's image backend does not validate the byte contents of Crossplane packages. As such, Crossplane does not detect if an attacker has tampered with a Package. The problem has been fixed in 1.11.5, 1.12.3 and 1.13.0. As a workaround, only use images from trusted sources and keep Package editing/creating privileges to administrators only.	8.3	More Details
CVE-2023-38669	Use after free in paddle.diagonal in PaddlePaddle before 2.5.0. This resulted in a potentially exploitable condition.	8.3	More Details
CVE-2023-32226	Sysaid - CWE-552: Files or Directories Accessible to External Parties - Authenticated users may exfiltrate files from the server via an unspecified method.	8.3	More Details
CVE-2023-38671	Heap buffer overflow in paddle.trace in PaddlePaddle before 2.5.0. This flaw can lead to a denial of service, information disclosure, or more damage is possible.	8.3	More Details
CVE-2023-37496	HCL Verse is susceptible to a Stored Cross Site Scripting (XSS) vulnerability. An attacker could execute script in a victim's web browser to perform operations as the victim and/or steal the victim's cookies, session tokens, or other sensitive information.	8.3	More Details
CVE-2023-34360	A stored cross-site scripting (XSS) issue was discovered within the Custom User Icons functionality of ASUS RT-AX88U running firmware versions 3.0.0.4.388.23110 and prior. After a remote attacker logging in device with regular user privilege, the remote attacker can perform a Stored Cross-site Scripting (XSS) attack by uploading image which containing JavaScript code.	8.2	More Details
CVE-2023-32443	An out-of-bounds read was addressed with improved input validation. This issue is fixed in macOS Monterey 12.6.8, macOS Ventura 13.5, macOS Big Sur 11.7.9. Processing a file may lead to a denial-of-service or potentially disclose memory contents.	8.1	More Details

CVE Number	Description	Base Score	Reference
CVE-2023-38510	Tolgee is an open-source localization platform. Starting in version 3.14.0 and prior to version 3.23.1, when a request is made using an API key, the backend fails to verify the permission scopes associated with the key, effectively bypassing permission checks entirely for some endpoints. It's important to note that this vulnerability only affects projects that have inadvertently exposed their API keys on the internet. Projects that have kept their API keys secure are not impacted. This issue is fixed in version 3.23.1.	8.1	More Details
CVE-2023-34551	In certain EZVIZ products, two stack buffer overflows in netClientSetWlanCfg function of the EZVIZ SDK command server can allow an authenticated attacker present on the same local network as the camera to achieve remote code execution. This affects CS-C6N-B0-1G2WF Firmware versions before V5.3.0 build 230215 and CS-C6N-R101-1G2WF Firmware versions before V5.3.0 build 230215 and CS-CV310-A0-1B2WFR Firmware versions before V5.3.0 build 230221 and CS-CV310-A0-1C2WFR-C Firmware versions before V5.3.2 build 230221 and CS-C6N-A0-1C2WFR-MUL Firmware versions before V5.3.2 build 230218 and CS-CV310-A0-3C2WFRL-1080p Firmware versions before V5.2.7 build 230302 and CS-CV310-A0-1C2WFR Wifi IP66 2.8mm 1080p Firmware versions before V5.3.2 build 230214 and CS-CV248-A0-32WMFR Firmware versions before V5.2.3 build 230217 and EZVIZ LC1C Firmware versions before V5.3.4 build 230214. The impact is: execute arbitrary code (remote).	8.0	More Details
CVE-2023-38424	The issue was addressed with improved memory handling. This issue is fixed in iOS 16.6 and iPadOS 16.6, macOS Ventura 13.5. An app may be able to execute arbitrary code with kernel privileges.	7.8	More Details
CVE-2023-35993	A use-after-free issue was addressed with improved memory management. This issue is fixed in macOS Monterey 12.6.8, iOS 15.7.8 and iPadOS 15.7.8, iOS 16.6 and iPadOS 16.6, tvOS 16.6, macOS Big Sur 11.7.9, macOS Ventura 13.5, watchOS 9.6. An app may be able to execute arbitrary code with kernel privileges.	7.8	More Details
CVE-2023-31427	Brocade Fabric OS versions before Brocade Fabric OS v9.1.1c, and v9.2.0 Could allow an authenticated, local user with knowledge of full path names inside Brocade Fabric OS to execute any command regardless of assigned privilege. Starting with Fabric OS v9.1.0, “root” account access is disabled.	7.8	More Details
CVE-2022-43701	When the installation directory does not have sufficiently restrictive file permissions, an attacker can modify files in the installation directory to cause execution of malicious code.	7.8	More Details

CVE Number	Description	Base Score	Reference
CVE-2022-43702	When the directory containing the installer does not have sufficiently restrictive file permissions, an attacker can modify (or replace) the installer to execute malicious code.	7.8	More Details
CVE-2022-43703	An installer that loads or executes files using an unconstrained search path may be vulnerable to substitute files under control of an attacker being loaded or executed instead of the intended files.	7.8	More Details
CVE-2023-36351	An issue in Viatom Health ViHealth for Android v.2.74.58 and before allows a remote attacker to execute arbitrary code via the com.viatom.baselib.mvvm.webWebViewActivity component.	7.8	More Details
CVE-2023-38136	The issue was addressed with improved memory handling. This issue is fixed in iOS 16.6 and iPadOS 16.6, watchOS 9.6. An app may be able to execute arbitrary code with kernel privileges.	7.8	More Details
CVE-2023-31425	A vulnerability in the fosexec command of Brocade Fabric OS after Brocade Fabric OS v9.1.0 and, before Brocade Fabric OS v9.1.1 could allow a local authenticated user to perform privilege escalation to root by breaking the rbash shell. Starting with Fabric OS v9.1.0, “root” account access is disabled.	7.8	More Details
CVE-2023-38261	The issue was addressed with improved memory handling. This issue is fixed in iOS 16.6 and iPadOS 16.6, macOS Ventura 13.5. An app may be able to execute arbitrary code with kernel privileges.	7.8	More Details
CVE-2023-38580	The issue was addressed with improved memory handling. This issue is fixed in iOS 16.6 and iPadOS 16.6, macOS Ventura 13.5, watchOS 9.6. An app may be able to execute arbitrary code with kernel privileges.	7.8	More Details
CVE-2023-32629	Local privilege escalation vulnerability in Ubuntu Kernels overlayfs ovl_copy_up_meta_inode_data skip permission checks when calling ovl_do_setxattr on Ubuntu kernels	7.8	More Details
CVE-2023-39147	An arbitrary file upload vulnerability in Uvdesk 1.1.3 allows attackers to execute arbitrary code via uploading a crafted image file.	7.8	More Details
CVE-2023-38565	A path handling issue was addressed with improved validation. This issue is fixed in macOS Monterey 12.6.8, iOS 16.6 and iPadOS 16.6, macOS Big Sur 11.7.9, macOS Ventura 13.5, watchOS 9.6. An app may be able to gain root privileges.	7.8	More Details
CVE-2023-32734	The issue was addressed with improved memory handling. This issue is fixed in iOS 16.6 and iPadOS 16.6, tvOS 16.6, macOS Ventura 13.5, watchOS 9.6. An app may be able to execute arbitrary code with kernel privileges.	7.8	More Details

CVE Number	Description	Base Score	Reference
CVE-2023-2640	On Ubuntu kernels carrying both c914c0e27eb0 and "UBUNTU: SAUCE: overlayfs: Skip permission checking for trusted.overlayfs.* xattrs", an unprivileged user may set privileged extended attributes on the mounted files, leading them to be set on the upper files without the appropriate security checks.	7.8	More Details
CVE-2023-32381	A use-after-free issue was addressed with improved memory management. This issue is fixed in macOS Monterey 12.6.8, iOS 16.6 and iPadOS 16.6, tvOS 16.6, macOS Big Sur 11.7.9, macOS Ventura 13.5, watchOS 9.6. An app may be able to execute arbitrary code with kernel privileges.	7.8	More Details
CVE-2021-31680	Deserialization of Untrusted Data vulnerability in yolo 5 allows attackers to execute arbitrary code via crafted yaml file.	7.8	More Details
CVE-2023-32418	The issue was addressed with improved checks. This issue is fixed in macOS Monterey 12.6.8, macOS Ventura 13.5, macOS Big Sur 11.7.9. Processing a file may lead to unexpected app termination or arbitrary code execution.	7.8	More Details
CVE-2023-38410	The issue was addressed with improved checks. This issue is fixed in iOS 16.6 and iPadOS 16.6, macOS Ventura 13.5. A user may be able to elevate privileges.	7.8	More Details
CVE-2023-4004	A use-after-free flaw was found in the Linux kernel's netfilter in the way a user triggers the nft_pipapo_remove function with the element, without a NFT_SET_EXT_KEY_END. This issue could allow a local user to crash the system or potentially escalate their privileges on the system.	7.8	More Details
CVE-2023-4033	OS Command Injection in GitHub repository mlflow/mlflow prior to 2.6.0.	7.8	More Details
CVE-2023-36854	The issue was addressed with improved checks. This issue is fixed in macOS Monterey 12.6.8, macOS Ventura 13.5, macOS Big Sur 11.7.9. Processing a file may lead to unexpected app termination or arbitrary code execution.	7.8	More Details
CVE-2023-32433	A use-after-free issue was addressed with improved memory management. This issue is fixed in macOS Monterey 12.6.8, iOS 15.7.8 and iPadOS 15.7.8, iOS 16.6 and iPadOS 16.6, tvOS 16.6, macOS Big Sur 11.7.9, macOS Ventura 13.5, watchOS 9.6. An app may be able to execute arbitrary code with kernel privileges.	7.8	More Details

CVE Number	Description	Base Score	Reference
CVE-2023-34634	Greenshot 1.2.10 and below allows arbitrary code execution because .NET content is insecurely deserialized when a .greenshot file is opened.	7.8	More Details
CVE-2023-30577	AMANDA (Advanced Maryland Automatic Network Disk Archiver) before tag-community-3.5.4 mishandles argument checking for runtar.c, a different vulnerability than CVE-2022-37705.	7.8	More Details
CVE-2023-26911	ASUS SetupAsusServices v1.0.5.1 in Asus Armoury Crate v5.3.4.0 contains an unquoted service path vulnerability which allows local users to launch processes with elevated privileges.	7.8	More Details
CVE-2020-10962	In PowerShell App Deployment Toolkit (aka PSAppDeployToolkit) through 3.8.0, an incorrect access control vulnerability in the default configuration may allow an authenticated user to potentially enable escalation of privilege via local access.	7.8	More Details
CVE-2023-32441	The issue was addressed with improved memory handling. This issue is fixed in macOS Monterey 12.6.8, iOS 15.7.8 and iPadOS 15.7.8, iOS 16.6 and iPadOS 16.6, tvOS 16.6, macOS Big Sur 11.7.9, macOS Ventura 13.5, watchOS 9.6. An app may be able to execute arbitrary code with kernel privileges.	7.8	More Details
CVE-2021-31681	Deserialization of Untrusted Data vulnerability in yolo 3 allows attackers to execute arbitrary code via crafted yaml file.	7.8	More Details
CVE-2023-3442	A missing authorization vulnerability exists in versions of the Jenkins Plug-in for ServiceNow DevOps prior to 1.38.1 that, if exploited successfully, could cause the unwanted exposure of sensitive information. To address this issue, apply the 1.38.1 version of the Jenkins plug-in for ServiceNow DevOps on your Jenkins server. No changes are required on your instances of the Now Platform.	7.7	More Details
CVE-2020-22623	Directory traversal vulnerability in Jinfornet Jreport 15.6 allows unauthenticated attackers to gain sensitive information.	7.5	More Details
CVE-2023-36983	LavaLite CMS v 9.0.0 is vulnerable to Sensitive Data Exposure.	7.5	More Details
CVE-2023-36984	LavaLite CMS v 9.0.0 is vulnerable to Sensitive Data Exposure.	7.5	More Details

CVE Number	Description	Base Score	Reference
CVE-2023-33742	TeleAdapt RoomCast TA-2400 1.0 through 3.1 suffers from Cleartext Storage of Sensitive Information: RSA private key in Update.exe.	7.5	More Details
CVE-2023-38571	This issue was addressed with improved validation of symlinks. This issue is fixed in macOS Big Sur 11.7.9, macOS Monterey 12.6.8, macOS Ventura 13.5. An app may be able to bypass Privacy preferences.	7.5	More Details
CVE-2023-26139	Versions of the package underscore-keypath from 0.0.11 are vulnerable to Prototype Pollution via the name argument of the setProperty() function. Exploiting this vulnerability is possible due to improper input sanitization which allows the usage of arguments like “__proto__”.	7.5	More Details
CVE-2023-38505	DietPi-Dashboard is a web dashboard for the operating system DietPi. The dashboard only allows for one TLS handshake to be in process at a given moment. Once a TCP connection is established in HTTPS mode, it will assume that it should be waiting for a handshake, and will stay this way indefinitely until a handshake starts or some error occurs. In version 0.6.1, this can be exploited by simply not starting the handshake, preventing any other TLS handshakes from getting through. An attacker can lock the dashboard in a state where it is waiting for a TLS handshake from the attacker, who won't provide it. This prevents any legitimate traffic from getting to the dashboard, and can last indefinitely. Version 0.6.2 has a patch for this issue. As a workaround, do not use HTTPS mode on the open internet where anyone can connect. Instead, put a reverse proxy in front of the dashboard, and have it handle any HTTPS connections.	7.5	More Details
CVE-2023-38504	Sails is a realtime MVC Framework for Node.js. In Sails apps prior to version 1.5.7,, an attacker can send a virtual request that will cause the node process to crash. This behavior was fixed in Sails v1.5.7. As a workaround, disable the sockets hook and remove the `sails.io.js` client.	7.5	More Details
CVE-2023-32444	A logic issue was addressed with improved validation. This issue is fixed in macOS Big Sur 11.7.9, macOS Monterey 12.6.8, macOS Ventura 13.5. A sandboxed process may be able to circumvent sandbox restrictions.	7.5	More Details
CVE-2023-4051	A website could have obscured the full screen notification by using the file open dialog. This could have led to user confusion and possible spoofing attacks. This vulnerability affects Firefox < 116, Firefox ESR < 115.2, and Thunderbird < 115.2.	7.5	More Details

CVE Number	Description	Base Score	Reference
CVE-2023-3825	PTC's KEPServerEX Versions 6.0 to 6.14.263 are vulnerable to being made to read a recursively defined object that leads to uncontrolled resource consumption. KEPServerEX uses OPC UA, a protocol which defines various object types that can be nested to create complex arrays. It does not implement a check to see if such an object is recursively defined, so an attack could send a maliciously created message that the decoder would try to decode until the stack overflowed and the device crashed.	7.5	More Details
CVE-2023-38750	In Zimbra Collaboration (ZCS) 8 before 8.8.15 Patch 41, 9 before 9.0.0 Patch 34, and 10 before 10.0.2, internal JSP and XML files can be exposed.	7.5	More Details
CVE-2023-38601	This issue was addressed by removing the vulnerable code. This issue is fixed in macOS Big Sur 11.7.9, macOS Monterey 12.6.8, macOS Ventura 13.5. An app may be able to modify protected parts of the file system.	7.5	More Details
CVE-2023-34359	ASUS RT-AX88U's httpd is subject to an unauthenticated DoS condition. A remote attacker can send a specially crafted request to the device which causes the httpd binary to crash within the "do_json_decode()" function of ej.c, resulting in a DoS condition.	7.5	More Details
CVE-2023-34358	ASUS RT-AX88U's httpd is subject to an unauthenticated DoS condition. A remote attacker can send a specially crafted request to a device which contains a specific user agent, causing the httpd binary to crash during a string comparison performed within web.c, resulting in a DoS condition.	7.5	More Details
CVE-2023-24971	IBM B2B Advanced Communications 1.0.0.0 and IBM Multi-Enterprise Integration Gateway 1.0.0.1 could allow a user to cause a denial of service due to the deserializing of untrusted serialized Java objects. IBM X-Force ID: 246976.	7.5	More Details
CVE-2023-37218	Tadiran Telecom Aeonix - CWE-22 Improper Limitation of a Pathname to a Restricted Directory ('Path Traversal')	7.5	More Details
CVE-2023-37216	AnaSystem SensMini M4 – Using the configuration tool, an authenticated user can cause Denial of Service for the device	7.5	More Details
CVE-2023-4048	An out-of-bounds read could have led to an exploitable crash when parsing HTML with DOMParser in low memory situations. This vulnerability affects Firefox < 116, Firefox ESR < 102.14, and Firefox ESR < 115.1.	7.5	More Details

CVE Number	Description	Base Score	Reference
CVE-2023-4055	When the number of cookies per domain was exceeded in `document.cookie`, the actual cookie jar sent to the host was no longer consistent with expected cookie jar state. This could have caused requests to be sent with some cookies missing. This vulnerability affects Firefox < 116, Firefox ESR < 102.14, and Firefox ESR < 115.1.	7.5	More Details
CVE-2023-4050	In some cases, an untrusted input stream was copied to a stack buffer without checking its size. This resulted in a potentially exploitable crash which could have led to a sandbox escape. This vulnerability affects Firefox < 116, Firefox ESR < 102.14, and Firefox ESR < 115.1.	7.5	More Details
CVE-2023-38609	An injection issue was addressed with improved input validation. This issue is fixed in macOS Ventura 13.5. An app may be able to bypass certain Privacy preferences.	7.5	More Details
CVE-2023-37478	pnpm is a package manager. It is possible to construct a tarball that, when installed via npm or parsed by the registry is safe, but when installed via pnpm is malicious, due to how pnpm parses tar archives. This can result in a package that appears safe on the npm registry or when installed via npm being replaced with a compromised or malicious version when installed via pnpm. This issue has been patched in version(s) 7.33.4 and 8.6.8.	7.5	More Details
CVE-2023-38564	The issue was addressed with improved checks. This issue is fixed in macOS Ventura 13.5. An app may be able to modify protected parts of the file system.	7.5	More Details
CVE-2023-38433	Fujitsu Real-time Video Transmission Gear "IP series" use hard-coded credentials, which may allow a remote unauthenticated attacker to initialize or reboot the products, and as a result, terminate the video transmission. Affected products and versions are as follows: IP-HE950E firmware versions V01L001 to V01L053, IP-HE950D firmware versions V01L001 to V01L053, IP-HE900E firmware versions V01L001 to V01L010, IP-HE900D firmware versions V01L001 to V01L004, IP-900E / IP-920E firmware versions V01L001 to V02L061, IP-900D / IP-900IID / IP-920D firmware versions V01L001 to V02L061, IP-90 firmware versions V01L001 to V01L013, and IP-9610 firmware versions V01L001 to V02L007.	7.5	More Details
CVE-2023-38572	The issue was addressed with improved checks. This issue is fixed in iOS 15.7.8 and iPadOS 15.7.8, iOS 16.6 and iPadOS 16.6, tvOS 16.6, macOS Ventura 13.5, Safari 16.6, watchOS 9.6. A website may be able to bypass Same Origin Policy.	7.5	More Details

CVE Number	Description	Base Score	Reference
CVE-2023-38603	The issue was addressed with improved checks. This issue is fixed in iOS 16.6 and iPadOS 16.6, macOS Ventura 13.5. A remote user may be able to cause a denial-of-service.	7.5	More Details
CVE-2022-43713	Interactive Forms (IAF) in GX Software XperienCentral versions 10.33.1 until 10.35.0 was vulnerable to invalid data input because form validation could be bypassed.	7.5	More Details
CVE-2023-38285	Trustwave ModSecurity 3.x before 3.0.10 has Inefficient Algorithmic Complexity.	7.5	More Details
CVE-2023-3107	A set of carefully crafted ipv6 packets can trigger an integer overflow in the calculation of a fragment reassembled packet's payload length field. This allows an attacker to trigger a kernel panic, resulting in a denial of service.	7.5	More Details
CVE-2023-30367	Multi-Remote Next Generation Connection Manager (mRemoteNG) is free software that enables users to store and manage multi-protocol connection configurations to remotely connect to systems. mRemoteNG configuration files can be stored in an encrypted state on disk. mRemoteNG version <= v1.76.20 and <= 1.77.3-dev loads configuration files in plain text into memory (after decrypting them if necessary) at application start-up, even if no connection has been established yet. This allows attackers to access contents of configuration files in plain text through a memory dump and thus compromise user credentials when no custom password encryption key has been set. This also bypasses the connection configuration file encryption setting by dumping already decrypted configurations from memory.	7.5	More Details
CVE-2022-4608	A vulnerability exists in HCI IEC 60870-5-104 function included in certain versions of the RTU500 series product. The vulnerability can only be exploited, if the HCI 60870-5-104 is configured with support for IEC 62351-3. After session resumption interval is expired an RTU500 initiated update of session parameters causes an unexpected restart due to a stack overflow.	7.5	More Details

CVE Number	Description	Base Score	Reference
CVE-2022-2502	A vulnerability exists in the HCI IEC 60870-5-104 function included in certain versions of the RTU500 series product. The vulnerability can only be exploited, if the HCI 60870-5-104 is configured with support for IEC 62351-5 and the CMU contains the license feature ‘Advanced security’ which must be ordered separately. If these preconditions are fulfilled, an attacker could exploit the vulnerability by sending a specially crafted message to the RTU500, causing the targeted RTU500 CMU to reboot. The vulnerability is caused by a missing input data validation which eventually if exploited causes an internal buffer to overflow in the HCI IEC 60870-5-104 function.	7.5	More Details
CVE-2022-43831	IBM Storage Scale Container Native Storage Access 5.1.2.1 through 5.1.6.1 could allow a local user to obtain escalated privileges on a host without proper security context settings configured. IBM X-Force ID: 238941.	7.4	More Details
CVE-2023-37219	Tadiran Telecom Composit - CWE-1236: Improper Neutralization of Formula Elements in a CSV File	7.3	More Details
CVE-2023-38489	Kirby is a content management system. A vulnerability in versions prior to 3.5.8.3, 3.6.6.3, 3.7.5.2, 3.8.4.1, and 3.9.6 affects all Kirby sites with user accounts (unless Kirby's API and Panel are disabled in the config). It can only be abused if a Kirby user is logged in on a device or browser that is shared with potentially untrusted users or if an attacker already maliciously used a previous password to log in to a Kirby site as the affected user. Insufficient Session Expiration is when a web site permits an attacker to reuse old session credentials or session IDs for authorization. In the variation described in this advisory, it allows attackers to stay logged in to a Kirby site on another device even if the logged in user has since changed their password. Kirby did not invalidate user sessions that were created with a password that was since changed by the user or by a site admin. If a user changed their password to lock out an attacker who was already in possession of the previous password or of a login session on another device or browser, the attacker would not be reliably prevented from accessing the Kirby site as the affected user. The problem has been patched in Kirby 3.5.8.3, 3.6.6.3, 3.7.5.2, 3.8.4.1, and 3.9.6. In all of the mentioned releases, the maintainers have updated the authentication implementation to keep track of the hashed password in each active session. If the password changed since the login, the session is invalidated. To enforce this fix even if the vulnerability was previously abused, all users are logged out from the Kirby site after updating to one of the patched releases.	7.3	More Details

CVE Number	Description	Base Score	Reference
CVE-2023-3985	A vulnerability has been found in SourceCodester Online Jewelry Store 1.0 and classified as critical. This vulnerability affects unknown code of the file login.php. The manipulation of the argument username/password leads to sql injection. The attack can be initiated remotely. The exploit has been disclosed to the public and may be used. VDB-235606 is the identifier assigned to this vulnerability.	7.3	More Details
CVE-2023-3670	In CODESYS Development System 3.5.9.0 to 3.5.17.0 and CODESYS Scripting 4.0.0.0 to 4.1.0.0 unsafe directory permissions would allow an attacker with local access to the workstation to place potentially harmful and disguised scripts that could be executed by legitimate users.	7.3	More Details
CVE-2023-23843	The SolarWinds Platform was susceptible to the Incorrect Comparison Vulnerability. This vulnerability allows users with administrative access to SolarWinds Web Console to execute arbitrary commands.	7.2	More Details
CVE-2023-33225	The SolarWinds Platform was susceptible to the Incorrect Comparison Vulnerability. This vulnerability allows users with administrative access to SolarWinds Web Console to execute arbitrary commands with SYSTEM privileges.	7.2	More Details
CVE-2023-23842	The SolarWinds Network Configuration Manager was susceptible to the Directory Traversal Vulnerability. This vulnerability allows users with administrative access to SolarWinds Web Console to execute arbitrary commands.	7.2	More Details
CVE-2023-35019	IBM Security Verify Governance, Identity Manager 10.0 could allow a remote authenticated attacker to execute arbitrary commands on the system by sending a specially crafted request. IBM X-Force ID: 257873.	7.2	More Details
CVE-2023-2685	A vulnerability was found in AO-OPC server versions mentioned above. As the directory information for the service entry is not enclosed in quotation marks, potential attackers could possibly call up another application than the AO-OPC server by starting the service. The service might be started with system user privileges which could cause a shift in user access privileges. It is unlikely to exploit the vulnerability in well maintained Windows installations since the attacker would need write access to system folders. An update is available that resolves the vulnerability found during an internal review in the product AO-OPC = 3.2.1	7.2	More Details
CVE-2023-31932	Sql injection vulnerability found in Rail Pass Management System v.1.0 allows a remote attacker to execute arbitrary code via the viewid parameter of the view-enquiry.php file.	7.2	More Details

CVE Number	Description	Base Score	Reference
CVE-2023-23844	The SolarWinds Platform was susceptible to the Incorrect Comparison Vulnerability. This vulnerability allows users with administrative access to SolarWinds Web Console to execute arbitrary commands with SYSTEM privileges.	7.2	More Details
CVE-2023-33224	The SolarWinds Platform was susceptible to the Incorrect Behavior Order Vulnerability. This vulnerability allows users with administrative access to SolarWinds Web Console to execute arbitrary commands with NETWORK SERVICE privileges.	7.2	More Details
CVE-2023-31933	Sql injection vulnerability found in Rail Pass Management System v.1.0 allows a remote attacker to execute arbitrary code via the editid parameter of the edit-pass-detail.php file.	7.2	More Details
CVE-2023-38425	The issue was addressed with improved memory handling. This issue is fixed in iOS 16.6 and iPadOS 16.6, macOS Ventura 13.5. An app may be able to execute arbitrary code with kernel privileges.	7.2	More Details
CVE-2023-31936	Sql injection vulnerability found in Rail Pass Management System v.1.0 allows a remote attacker to execute arbitrary code via the viewid parameter of the view-pass-detail.php file.	7.2	More Details
CVE-2023-31937	Sql injection vulnerability found in Rail Pass Management System v.1.0 allows a remote attacker to execute arbitrary code via the editid parameter of the edit-cateogry-detail.php file.	7.2	More Details
CVE-2023-28130	Local user may lead to privilege escalation using Gaia Portal hostnames page.	7.2	More Details
CVE-2023-37977	Unauth. Reflected Cross-Site Scripting (XSS) vulnerability in WPFunnels Team Drag & Drop Sales Funnel Builder for WordPress – WPFunnels plugin <= 2.7.16 versions.	7.1	More Details
CVE-2023-37981	Unauth. Reflected Cross-Site Scripting (XSS) vulnerability in WPKube Authors List plugin <= 2.0.2 versions.	7.1	More Details
CVE-2023-37894	Unauth. Reflected Cross-Site Scripting (XSS) vulnerability in RadiusTheme Variation Images Gallery for WooCommerce plugin <= 2.3.3 versions.	7.1	More Details

CVE Number	Description	Base Score	Reference
CVE-2023-38488	Kirby is a content management system. A vulnerability in versions prior to 3.5.8.3, 3.6.6.3, 3.7.5.2, 3.8.4.1, and 3.9.6 affects all Kirby sites that might have potential attackers in the group of authenticated Panel users or that allow external visitors to update a Kirby content file (e.g. via a contact or comment form). Kirby sites are *not* affected if they don't allow write access for untrusted users or visitors. A field injection in a content storage implementation is a type of vulnerability that allows attackers with content write access to overwrite content fields that the site developer didn't intend to be modified. In a Kirby site this can be used to alter site content, break site behavior or inject malicious data or code. The exact security risk depends on the field type and usage. Kirby stores content of the site, of pages, files and users in text files by default. The text files use Kirby's KirbyData format where each field is separated by newlines and a line with four dashes (`----`). When reading a KirbyData file, the affected code first removed the Unicode BOM sequence from the file contents and afterwards split the content into fields by the field separator. When writing to a KirbyData file, field separators in field data are escaped to prevent user input from interfering with the field structure. However this escaping could be tricked by including a Unicode BOM sequence in a field separator (e.g. `--\xEF\xBB\xBF--`). When writing, this was not detected as a separator, but because the BOM was removed during reading, it could be abused by attackers to inject other field data into content files. Because each field can only be defined once per content file, this vulnerability only affects fields in the content file that were defined above the vulnerable user-writable field or not at all. Fields that are defined below the vulnerable field override the injected field content and were therefore already protected. The problem has been patched in Kirby 3.5.8.3, 3.6.6.3, 3.7.5.2, 3.8.4.1, and 3.9.6. In all of the mentioned releases, the maintainers have fixed the affected code to only remove the Unicode BOM sequence at the beginning of the file. This fixes this vulnerability both for newly written as well as for existing content files.	7.1	More Details
CVE-2023-37975	Unauth. Reflected Cross-Site Scripting (XSS) vulnerability in RadiusTheme Variation Swatches for WooCommerce plugin <= 2.3.7 versions.	7.1	More Details
CVE-2023-37976	Unauth. Reflected Cross-Site Scripting (XSS) vulnerability in Radio Forge Muses Player with Skins plugin <= 2.5 versions.	7.1	More Details
CVE-2023-37979	Unauth. Reflected Cross-Site Scripting (XSS) vulnerability in Saturday Drive Ninja Forms Contact Form plugin <= 3.6.25 versions.	7.1	More Details

CVE Number	Description	Base Score	Reference
CVE-2023-38490	Kirby is a content management system. A vulnerability in versions prior to 3.5.8.3, 3.6.6.3, 3.7.5.2, 3.8.4.1, and 3.9.6 only affects Kirby sites that use the `Xml` data handler (e.g. `Data::decode($string, 'xml')`) or the `Xml::parse()` method in site or plugin code. The Kirby core does not use any of the affected methods. XML External Entities (XXE) is a little used feature in the XML markup language that allows to include data from external files in an XML structure. If the name of the external file can be controlled by an attacker, this becomes a vulnerability that can be abused for various system impacts like the disclosure of internal or confidential data that is stored on the server (arbitrary file disclosure) or to perform network requests on behalf of the server (server-side request forgery, SSRF). Kirby's `Xml::parse()` method used PHP's `LIBXML_NOENT` constant, which enabled the processing of XML external entities during the parsing operation. The `Xml::parse()` method is used in the `Xml` data handler (e.g. `Data::decode($string, 'xml')`). Both the vulnerable method and the data handler are not used in the Kirby core. However they may be used in site or plugin code, e.g. to parse RSS feeds or other XML files. If those files are of an external origin (e.g. uploaded by a user or retrieved from an external URL), attackers may be able to include an external entity in the XML file that will then be processed in the parsing process. Kirby sites that don't use XML parsing in site or plugin code are *not* affected. The problem has been patched in Kirby 3.5.8.3, 3.6.6.3, 3.7.5.2, 3.8.4.1, and 3.9.6. In all of the mentioned releases, the maintainers have removed the `LIBXML_NOENT` constant as processing of external entities is out of scope of the parsing logic. This protects all uses of the method against the described vulnerability.	6.8	More Details
CVE-2023-37467	Discourse is an open source discussion platform. Prior to version 3.1.0.beta7 of the `beta` and `tests-passed` branches, a CSP (Content Security Policy) nonce reuse vulnerability was discovered could allow cross-site scripting (XSS) attacks to bypass CSP protection for anonymous (i.e. unauthenticated) users. There are no known XSS vectors at the moment, but should one be discovered, this vulnerability would allow the XSS attack to bypass CSP and execute successfully. This vulnerability isn't applicable to logged-in users. Version 3.1.0.beta7 contains a patch. The stable branch doesn't have this vulnerability. A workaround to prevent the vulnerability is to disable Google Tag Manager, i.e., unset the `gtm container id` setting.	6.8	More Details
CVE-2023-31426	The Brocade Fabric OS Commands “configupload” and “configdownload” before Brocade Fabric OS v9.1.1c, v8.2.3d, v9.2.0 print scp, sftp, ftp servers passwords in supportsave. This could allow a remote authenticated attacker to access sensitive information.	6.8	More Details

CVE Number	Description	Base Score	Reference
CVE-2023-28014	HCL BigFix Mobile is vulnerable to a cross-site scripting attack. An authenticated attacker could inject malicious scripts into the application.	6.6	More Details
CVE-2022-4925	Insufficient validation of untrusted input in QUIC in Google Chrome prior to 97.0.4692.71 allowed a remote attacker to perform header splitting via malicious network traffic. (Chromium security severity: Low)	6.5	More Details
CVE-2023-28013	HCL Verse is susceptible to a Reflected Cross Site Scripting (XSS) vulnerability. By tricking a user into entering crafted markup a remote, unauthenticated attacker could execute script in a victim's web browser to perform operations as the victim and/or steal the victim's cookies, session tokens, or other sensitive information.	6.5	More Details
CVE-2023-4053	A website could have obscured the full screen 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 < 116, Firefox ESR < 115.2, and Thunderbird < 115.2.	6.5	More Details
CVE-2022-4926	Insufficient policy enforcement in Intents in Google Chrome on Android prior to 109.0.5414.119 allowed a remote attacker to bypass same origin policy via a crafted HTML page. (Chromium security severity: Medium)	6.5	More Details
CVE-2023-2311	Insufficient policy enforcement in File System API in Google Chrome prior to 112.0.5615.49 allowed a remote attacker to bypass filesystem restrictions via a crafted HTML page. (Chromium security severity: Medium)	6.5	More Details
CVE-2023-4052	The Firefox updater created a directory writable by non-privileged users. When uninstalling Firefox, any files in that directory would be recursively deleted with the permissions of the uninstalling user account. This could be combined with creation of a junction (a form of symbolic link) to allow arbitrary file deletion controlled by the non-privileged user. *This bug only affects Firefox on Windows. Other operating systems are unaffected.* This vulnerability affects Firefox < 116, Firefox ESR < 115.1, and Thunderbird < 115.1.	6.5	More Details
CVE-2023-2314	Insufficient data validation in DevTools in Google Chrome prior to 111.0.5563.64 allowed a remote attacker to bypass navigation restrictions via a crafted HTML page. (Chromium security severity: Low)	6.5	More Details
CVE-2022-4913	Inappropriate implementation in Extensions in Google Chrome prior to 105.0.5195.52 allowed a remote attacker who had compromised the renderer process to spoof extension storage via a crafted HTML page. (Chromium security severity: High)	6.5	More Details

CVE Number	Description	Base Score	Reference
CVE-2023-38133	The issue was addressed with improved checks. This issue is fixed in iOS 15.7.8 and iPadOS 15.7.8, iOS 16.6 and iPadOS 16.6, tvOS 16.6, macOS Ventura 13.5, Safari 16.6, watchOS 9.6. Processing web content may disclose sensitive information.	6.5	More Details
CVE-2022-4888	The Checkout Fields Manager WordPress plugin before 1.0.2, Abandoned Cart Recovery WordPress plugin before 1.2.5, Custom Fields for WooCommerce WordPress plugin before 1.0.4, Custom Order Number WordPress plugin through 1.0.1, Custom Registration Forms Builder WordPress plugin before 1.0.2, Advanced Free Gifts WordPress plugin before 1.0.2, Gift Registry for WooCommerce WordPress plugin through 1.0.1, Image Watermark for WooCommerce WordPress plugin before 1.0.1, Order Approval for WooCommerce WordPress plugin before 1.1.0, Order Tracking for WooCommerce WordPress plugin before 1.0.2, Price Calculator for WooCommerce WordPress plugin through 1.0.3, Product Dynamic Pricing and Discounts WordPress plugin through 1.0.6, Product Labels and Stickers WordPress plugin through 1.0.1 have flawed CSRF checks in various places, which could allow attackers to make logged in users perform unwanted actions	6.5	More Details
CVE-2023-39152	Always-incorrect control flow implementation in Jenkins Gradle Plugin 2.8 may result in credentials not being masked (i.e., replaced with asterisks) in the build log in some circumstances.	6.5	More Details
CVE-2022-4911	Insufficient data validation in DevTools in Google Chrome prior to 106.0.5249.62 allowed a remote attacker to bypass content security policy via a crafted HTML page. (Chromium security severity: Low)	6.5	More Details
CVE-2023-39154	Incorrect permission checks in Jenkins Qualys Web App Scanning Connector Plugin 2.0.10 and earlier allow attackers with global Item/Configure permission to connect to an attacker-specified URL using attacker-specified credentials IDs obtained through another method, capturing credentials stored in Jenkins.	6.5	More Details
CVE-2023-35016	IBM Security Verify Governance, Identity Manager 10.0 could allow a remote attacker to traverse directories on the system. An attacker could send a specially crafted URL request containing "dot dot" sequences (/../) to view arbitrary files on the system. IBM X-Force ID: 257772.	6.5	More Details
CVE-2021-4324	Insufficient policy enforcement in Google Update in Google Chrome prior to 90.0.4430.93 allowed a remote attacker to read arbitrary files via a malicious file. (Chromium security severity: Medium)	6.5	More Details

CVE Number	Description	Base Score	Reference
CVE-2021-4323	Insufficient validation of untrusted input in Extensions in Google Chrome prior to 90.0.4430.72 allowed an attacker who convinced a user to install a malicious extension to access local files via a crafted Chrome Extension. (Chromium security severity: Medium)	6.5	More Details
CVE-2022-4915	Inappropriate implementation in URL Formatting in Google Chrome prior to 103.0.5060.134 allowed a remote attacker to perform domain spoofing via a crafted HTML page. (Chromium security severity: Medium)	6.5	More Details
CVE-2022-4922	Inappropriate implementation in Blink in Google Chrome prior to 99.0.4844.51 allowed a remote attacker to perform UI spoofing via a crafted HTML page. (Chromium security severity: Medium)	6.5	More Details
CVE-2020-21881	Cross Site Request Forgery (CSRF) vulnerability in admin.php in DuxCMS 2.1 allows remote attackers to modtify application data via article/admin/content/add.	6.5	More Details
CVE-2022-43712	POST requests to /web/mvc in GX Software XperienCentral version 10.36.0 and earlier were not blocked for uses that are not logged in. If an unauthorized user is able to bypass other security filters they are able to post unauthorized data to the server because of CVE-2022-22965.	6.5	More Details
CVE-2023-32654	A logic issue was addressed with improved state management. This issue is fixed in macOS Ventura 13.5. A user may be able to read information belonging to another user.	6.5	More Details
CVE-2023-37970	Auth. (contributor+) Stored Cross-Site Scripting (XSS) vulnerability in Matthew Fries MF Gig Calendar plugin <= 1.2 versions.	6.5	More Details
CVE-2023-37049	emlog 2.1.9 is vulnerable to Arbitrary file deletion via admin\template.php.	6.5	More Details
CVE-2023-38599	A logic issue was addressed with improved state management. This issue is fixed in Safari 16.6, watchOS 9.6, iOS 15.7.8 and iPadOS 15.7.8, tvOS 16.6, iOS 16.6 and iPadOS 16.6, macOS Ventura 13.5. A website may be able to track sensitive user information.	6.5	More Details
CVE-2023-20891	The VMware Tanzu Application Service for VMs and Isolation Segment contain an information disclosure vulnerability due to the logging of credentials in hex encoding in platform system audit logs. A malicious non-admin user who has access to the platform system audit logs can access hex encoded CF API admin credentials and can push new malicious versions of an application. In a default deployment non-admin users do not have access to the platform system audit logs.	6.5	More Details

CVE Number	Description	Base Score	Reference
CVE-2023-3508	The WooCommerce Pre-Orders WordPress plugin before 2.0.3 has a flawed CSRF check when processing its tab actions, which could allow attackers to make logged in admins email pre-orders customer, change the released date, mark all pre-orders of a specific product as complete or cancel via CSRF attacks	6.5	More Details
CVE-2023-3507	The WooCommerce Pre-Orders WordPress plugin before 2.0.3 has a flawed CSRF check when canceling pre-orders, which could allow attackers to make logged in admins cancel arbitrary pre-orders via a CSRF attack	6.5	More Details
CVE-2023-3345	The LMS by Masteriyo WordPress plugin before 1.6.8 does not have proper authorization in one some of its REST API endpoints, making it possible for any students to retrieve email addresses of other students	6.5	More Details
CVE-2023-3988	A vulnerability was found in Cafe Billing System 1.0. It has been declared as critical. Affected by this vulnerability is an unknown functionality of the file index.php of the component Order Handler. The manipulation of the argument id leads to sql injection. The attack can be launched remotely. The exploit has been disclosed to the public and may be used. The identifier VDB-235609 was assigned to this vulnerability.	6.3	More Details
CVE-2023-3987	A vulnerability was found in SourceCodester Simple Online Mens Salon Management System 1.0. It has been classified as critical. Affected is an unknown function of the file /admin/?page=user/manage_user&id=3. The manipulation of the argument id leads to sql injection. It is possible to launch the attack remotely. The exploit has been disclosed to the public and may be used. The identifier of this vulnerability is VDB-235608.	6.3	More Details
CVE-2023-3739	Insufficient validation of untrusted input in Chromad in Google Chrome on ChromeOS prior to 115.0.5790.131 allowed a remote attacker to execute arbitrary code via a crafted shell script. (Chromium security severity: Low)	6.3	More Details
CVE-2023-3984	A vulnerability, which was classified as critical, was found in phpscriptpoint RecipePoint 1.9. This affects an unknown part of the file /recipe-result. The manipulation of the argument text/category/type/difficulty/cuisine/cooking_method leads to sql injection. It is possible to initiate the attack remotely. The identifier VDB-235605 was assigned to this vulnerability.	6.3	More Details
CVE-2022-4909	Inappropriate implementation in XML in Google Chrome prior to 107.0.5304.62 allowed a remote attacker to potentially perform an ASLR bypass via a crafted HTML page. (Chromium security severity: Low)	6.3	More Details

CVE Number	Description	Base Score	Reference
CVE-2023-37215	JBL soundbar multibeam 5.1 - CWE-798: Use of Hard-coded Credentials	6.2	More Details
CVE-2023-34916	Fuge CMS v1.0 contains an Open Redirect vulnerability via /front/ProcessAct.java.	6.1	More Details
CVE-2022-43711	Interactive Forms (IAF) in GX Software XperienCentral versions 10.29.1 until 10.33.0 was vulnerable to cross site scripting attacks (XSS) because the CSP header uses eval() in the script-src.	6.1	More Details
CVE-2023-37580	Zimbra Collaboration (ZCS) 8 before 8.8.15 Patch 41 allows XSS in the Zimbra Classic Web Client.	6.1	More Details
CVE-2023-34917	Fuge CMS v1.0 contains an Open Redirect vulnerability in member/RegisterAct.java.	6.1	More Details
CVE-2023-3292	The grid-kit-premium WordPress plugin before 2.2.0 does not escape some parameters as well as generated URLs before outputting them in attributes, leading to Reflected Cross-Site Scripting which could be used against high privilege users such as admin	6.1	More Details
CVE-2022-31456	A cross-site scripting (XSS) vulnerability in Truedesk v1.2.2 allows attackers to execute arbitrary web scripts or HTML via a crafted payload injected into the team name parameter.	6.1	More Details
CVE-2023-3414	A cross-site request forgery vulnerability exists in versions of the Jenkins Plug-in for ServiceNow DevOps prior to 1.38.1 that, if exploited successfully, could cause the unwanted exposure of sensitive information. To address this issue, apply the 1.38.1 version of the Jenkins plug-in for ServiceNow DevOps on your Jenkins server. No changes are required on your instances of the Now Platform.	6.1	More Details
CVE-2023-3134	The Forminator WordPress plugin before 1.24.4 does not properly escape values that are being reflected inside form fields that use pre-populated query parameters, which could lead to reflected XSS attacks.	6.1	More Details
CVE-2023-38308	An issue was discovered in Webmin 2.021. A Cross-Site Scripting (XSS) vulnerability was discovered in the HTTP Tunnel functionality when handling third-party domain URLs. By providing a crafted URL from a third-party domain, an attacker can inject malicious code. leading to the execution of arbitrary JavaScript code within the context of the victim's browser.	6.1	More Details

CVE Number	Description	Base Score	Reference
CVE-2023-38306	An issue was discovered in Webmin 2.021. A Cross-site Scripting (XSS) Bypass vulnerability was discovered in the file upload functionality. Normally, the application restricts the upload of certain file types such as .svg, .php, etc., and displays an error message if a prohibited file type is detected. However, by following certain steps, an attacker can bypass these restrictions and inject malicious code.	6.1	More Details
CVE-2023-38305	An issue was discovered in Webmin 2.021. The download functionality allows an attacker to exploit a Cross-Site Scripting (XSS) vulnerability. By providing a crafted download path containing a malicious payload, an attacker can inject arbitrary code, which is then executed within the context of the victim's browser when the download link is accessed.	6.1	More Details
CVE-2023-35791	Vound Intella Connect 2.6.0.3 has an Open Redirect vulnerability.	6.1	More Details
CVE-2023-37624	Netdisco before v2.063000 was discovered to contain an open redirect vulnerability. An attacker may exploit this vulnerability to redirect users to arbitrary web URLs by tricking the victim users to click on crafted links.	6.1	More Details
CVE-2023-0602	The Twittee Text Tweet WordPress plugin through 1.0.8 does not properly escape POST values which are printed back to the user inside one of the plugin's administrative page, which allows reflected XSS attacks targeting administrators to happen.	6.1	More Details
CVE-2023-38309	An issue was discovered in Webmin 2.021. A Reflected Cross-Site Scripting (XSS) vulnerability was discovered in the package search functionality. The vulnerability allows an attacker to inject a malicious payload in the "Search for Package" field, which gets reflected back in the application's response, leading to the execution of arbitrary JavaScript code within the context of the victim's browser.	6.1	More Details
CVE-2023-3973	Cross-site Scripting (XSS) - Reflected in GitHub repository jgraph/drawio prior to 21.6.3.	6.1	More Details
CVE-2022-31455	* A cross-site scripting (XSS) vulnerability in Truedesk v1.2.2 allows attackers to execute arbitrary web scripts or HTML via a crafted payload injected into a user chat box.	6.1	More Details
CVE-2022-31200	Atmail 5.62 allows XSS via the mail/parse.php?file=html/$this-%3ELanguage/help/filexp.html&FirstLoad=1&HelpFile=file.html Search Terms field.	6.1	More Details

CVE Number	Description	Base Score	Reference
CVE-2023-32450	Dell Power Manager, Versions 3.3 to 3.14 contains an Improper Access Control vulnerability. A low-privileged malicious user may potentially exploit this vulnerability to perform arbitrary code execution with limited access.	6.1	More Details
CVE-2023-34869	PHPJabbers Catering System v1.0 was discovered to contain a cross-site scripting (XSS) vulnerability via the component /index.php?controller=pjAdmin&action=pjActionForgot.	6.1	More Details
CVE-2023-32445	This issue was addressed with improved checks. This issue is fixed in Safari 16.6, watchOS 9.6, iOS 15.7.8 and iPadOS 15.7.8, tvOS 16.6, iOS 16.6 and iPadOS 16.6, macOS Ventura 13.5. Processing a document may lead to a cross site scripting attack.	6.1	More Details
CVE-2022-31454	Yii 2 v2.0.45 was discovered to contain a cross-site scripting (XSS) vulnerability via the endpoint /books. NOTE: this is disputed by the vendor because the cve-2022-31454-8e8555c31fd3 page does not describe why /books has a relationship to Yii 2.	6.1	More Details
CVE-2023-33560	There is a Cross Site Scripting (XSS) vulnerability in "cid" parameter of preview.php in PHPJabbers Time Slots Booking Calendar v3.3.	6.1	More Details
CVE-2023-36942	A cross-site scripting (XSS) vulnerability in PHPGurukul Online Fire Reporting System Using PHP and MySQL 1.2 allows attackers to execute arbitrary web scripts or HTML via a crafted payload injected into the website title field.	6.1	More Details
CVE-2023-36941	A cross-site scripting (XSS) vulnerability in PHPGurukul Online Fire Reporting System Using PHP and MySQL 1.2 allows attackers to execute arbitrary web scripts or HTML via a crafted payload injected into the team name, leader, and member fields.	6.1	More Details
CVE-2023-33564	There is a Cross Site Scripting (XSS) vulnerability in the "theme" parameter of preview.php in PHPJabbers Time Slots Booking Calendar v3.3.	6.1	More Details
CVE-2021-36580	Open Redirect vulnerability exists in IceWarp MailServer IceWarp Server Deep Castle 2 Update 1 (13.0.1.2) via the referer parameter.	6.1	More Details
CVE-2023-4049	Race conditions in reference counting code were found through code inspection. These could have resulted in potentially exploitable use-after-free vulnerabilities. This vulnerability affects Firefox < 116, Firefox ESR < 102.14, and Firefox ESR < 115.1.	5.9	More Details

CVE Number	Description	Base Score	Reference
CVE-2023-37993	Auth. Stored Cross-Site Scripting (XSS) vulnerability in maennchen1.De wpShopGermany IT-RECHT KANZLEI plugin <= 1.7 versions.	5.9	More Details
CVE-2023-32427	This issue was addressed by using HTTPS when sending information over the network. This issue is fixed in Apple Music 4.2.0 for Android. An attacker in a privileged network position may be able to intercept network traffic.	5.9	More Details
CVE-2023-37980	Auth. (admin+) Stored Cross-Site Scripting (XSS) vulnerability in Gravity Master Custom Field For WP Job Manager plugin <= 1.1 versions.	5.9	More Details
CVE-2023-32468	Dell ECS Streamer, versions prior to 2.0.7.1, contain an insertion of sensitive information in log files vulnerability. A remote malicious high-privileged user could potentially exploit this vulnerability leading to exposure of this sensitive data.	5.8	More Details
CVE-2023-38491	Kirby is a content management system. A vulnerability in versions prior to 3.5.8.3, 3.6.6.3, 3.7.5.2, 3.8.4.1, and 3.9.6 affects all Kirby sites that might have potential attackers in the group of authenticated Panel users or that allow external visitors to upload an arbitrary file to the content folder. Kirby sites are not affected if they don't allow file uploads for untrusted users or visitors or if the file extensions of uploaded files are limited to a fixed safe list. The attack requires user interaction by another user or visitor and cannot be automated. An editor with write access to the Kirby Panel could upload a file with an unknown file extension like `.xyz` that contains HTML code including harmful content like `<script>` tags. The direct link to that file could be sent to other users or visitors of the site. If the victim opened that link in a browser where they are logged in to Kirby and the file had not been opened by anyone since the upload, Kirby would not be able to send the correct MIME content type, instead falling back to `text/html`. The browser would then run the script, which could for example trigger requests to Kirby's API with the permissions of the victim. The issue was caused by the underlying `Kirby\Http\Response::file()` method, which didn't have an explicit fallback if the MIME type could not be determined from the file extension. If you use this method in site or plugin code, these uses may be affected by the same vulnerability. The problem has been patched in Kirby 3.5.8.3, 3.6.6.3, 3.7.5.2, 3.8.4.1, and 3.9.6. In all of the mentioned releases, the maintainers have fixed the affected method to use a fallback MIME type of `text/plain` and set the `X-Content-Type-Options: nosniff` header if the MIME type of the file is unknown.	5.7	More Details
CVE-2023-38602	A permissions issue was addressed with additional restrictions. This issue is fixed in macOS Monterey 12.6.8, macOS Ventura 13.5, macOS Big Sur 11.7.9. An app may be able to modify protected parts of the file system.	5.5	More Details

CVE Number	Description	Base Score	Reference
CVE-2023-38560	An integer overflow flaw was found in pcl/pl/plfont.c:418 in pl_glyph_name in ghostscript. This issue may allow a local attacker to cause a denial of service via transforming a crafted PCL file to PDF format.	5.5	More Details
CVE-2023-38421	The issue was addressed with improved checks. This issue is fixed in macOS Ventura 13.5, macOS Monterey 12.6.8. Processing a 3D model may result in disclosure of process memory.	5.5	More Details
CVE-2023-38593	A logic issue was addressed with improved checks. This issue is fixed in macOS Monterey 12.6.8, iOS 16.6 and iPadOS 16.6, macOS Big Sur 11.7.9, macOS Ventura 13.5, watchOS 9.6. An app may be able to cause a denial-of-service.	5.5	More Details
CVE-2023-31429	Brocade Fabric OS before Brocade Fabric OS 9.1.1c, 9.2.0 contains a vulnerability when using various commands such as “chassisdistribute”, “reboot”, “rasman”, errmoduleshow, errfilterset, hassiscfgperrthreshold, supportshowcfgdisable and supportshowcfgenable commands that can cause the content of shell interpreted variables to be printed in the terminal.	5.5	More Details
CVE-2023-38608	The issue was addressed with additional permissions checks. This issue is fixed in macOS Ventura 13.5. An app may be able to access user-sensitive data.	5.5	More Details
CVE-2023-28203	The issue was addressed with improved checks. This issue is fixed in Apple Music 4.2.0 for Android. An app may be able to access contacts.	5.5	More Details
CVE-2023-38259	A logic issue was addressed with improved restrictions. This issue is fixed in macOS Monterey 12.6.8, macOS Ventura 13.5, macOS Big Sur 11.7.9. An app may be able to access user-sensitive data.	5.5	More Details
CVE-2023-38559	A buffer overflow flaw was found in base/gdevdevn.c:1973 in devn_pcx_write_rle() in ghostscript. This issue may allow a local attacker to cause a denial of service via outputting a crafted PDF file for a DEVN device with gs.	5.5	More Details
CVE-2023-34872	A vulnerability in Outline.cc for Poppler prior to 23.06.0 allows a remote attacker to cause a Denial of Service (DoS) (crash) via a crafted PDF file in OutlineItem::open.	5.5	More Details

CVE Number	Description	Base Score	Reference
CVE-2023-32416	A logic issue was addressed with improved restrictions. This issue is fixed in macOS Monterey 12.6.8, iOS 15.7.8 and iPadOS 15.7.8, iOS 16.6 and iPadOS 16.6, macOS Ventura 13.5, watchOS 9.6. An app may be able to read sensitive location information.	5.5	More Details
CVE-2023-35983	This issue was addressed with improved data protection. This issue is fixed in macOS Monterey 12.6.8, macOS Ventura 13.5, macOS Big Sur 11.7.9. An app may be able to modify protected parts of the file system.	5.5	More Details
CVE-2023-37732	Yasm v1.3.0.78 was found prone to NULL Pointer Dereference in /libyasm/intnum.c and /elf/elf.c, which allows the attacker to cause a denial of service via a crafted file.	5.5	More Details
CVE-2023-4054	When opening appref-ms files, Firefox did not warn the user that these files may contain malicious code. *This bug only affects Firefox on Windows. Other operating systems are unaffected.* This vulnerability affects Firefox < 116, Firefox ESR < 102.14, Firefox ESR < 115.1, Thunderbird < 102.14, and Thunderbird < 115.1.	5.5	More Details
CVE-2023-38258	The issue was addressed with improved checks. This issue is fixed in macOS Ventura 13.5, macOS Monterey 12.6.8. Processing a 3D model may result in disclosure of process memory.	5.5	More Details
CVE-2023-33802	A buffer overflow in SumatraPDF Reader v3.4.6 allows attackers to cause a Denial of Service (DoS) via a crafted text file.	5.5	More Details
CVE-2023-32429	The issue was addressed with improved checks. This issue is fixed in macOS Ventura 13.5. An app may be able to bypass Privacy preferences.	5.5	More Details
CVE-2023-32442	An access issue was addressed with improved access restrictions. This issue is fixed in macOS Ventura 13.5, macOS Monterey 12.6.8. A shortcut may be able to modify sensitive Shortcuts app settings.	5.5	More Details
CVE-2023-38606	This issue was addressed with improved state management. This issue is fixed in macOS Monterey 12.6.8, iOS 15.7.8 and iPadOS 15.7.8, iOS 16.6 and iPadOS 16.6, tvOS 16.6, macOS Big Sur 11.7.9, macOS Ventura 13.5, watchOS 9.6. An app may be able to modify sensitive kernel state. Apple is aware of a report that this issue may have been actively exploited against versions of iOS released before iOS 15.7.1.	5.5	More Details
CVE-2023-36862	A downgrade issue affecting Intel-based Mac computers was addressed with additional code-signing restrictions. This issue is fixed in macOS Ventura 13.5. An app may be able to determine a user's current location.	5.5	More Details

CVE Number	Description	Base Score	Reference
CVE-2020-36763	Cross Site Scripting (XSS) vulnerability in DuxCMS 2.1 allows remote attackers to run arbitrary code via the content, time, copyfrom parameters when adding or editing a post.	5.4	More Details
CVE-2023-38512	Cross-Site Request Forgery (CSRF) vulnerability in Wpstream WpStream – Live Streaming, Video on Demand, Pay Per View plugin <= 4.5.4 versions.	5.4	More Details
CVE-2023-3946	A reflected cross-site scripting (XSS) vulnerability in ePO prior to 5.10 SP1 Update 1allows a remote unauthenticated attacker to potentially obtain access to an ePO administrator's session by convincing the authenticated ePO administrator to click on a carefully crafted link. This would lead to limited access to sensitive information and limited ability to alter some information in ePO.	5.4	More Details
CVE-2023-28012	HCL BigFix Mobile is vulnerable to a command injection attack. An authenticated attacker could run arbitrary shell commands on the WebUI server.	5.4	More Details
CVE-2022-4910	Inappropriate implementation in Autofill in Google Chrome prior to 107.0.5304.62 allowed a remote attacker to bypass navigation restrictions via a crafted HTML page. (Chromium security severity: Medium)	5.4	More Details
CVE-2023-38310	An issue was discovered in Webmin 2.021. A Stored Cross-Site Scripting (XSS) vulnerability was discovered in the configuration settings of the system logs functionality. The vulnerability allows an attacker to store an XSS payload in the configuration settings of specific log files. This results in the execution of that payload whenever the affected log files are accessed.	5.4	More Details
CVE-2023-31466	An XSS issue was discovered in FSMLabs TimeKeeper 8.0.17. On the "Configuration -> Compliance -> Add a new compliance report" and "Configuration -> Timekeeper Configuration -> Add a new source there" screens, there are entry points to inject JavaScript code.	5.4	More Details
CVE-2023-23548	Reflected XSS in business intelligence in Checkmk <2.2.0p8, <2.1.0p32, <2.0.0p38, <=1.6.0p30.	5.4	More Details
CVE-2023-38311	An issue was discovered in Webmin 2.021. A Stored Cross-Site Scripting (XSS) vulnerability was discovered in the System Logs Viewer functionality. The vulnerability allows an attacker to store a malicious payload in the configuration field, triggering the execution of the payload when saving the configuration or when accessing the System Logs Viewer page.	5.4	More Details

CVE Number	Description	Base Score	Reference
CVE-2023-36211	The Barebones CMS v2.0.2 is vulnerable to Stored Cross-Site Scripting (XSS) when an authenticated user interacts with certain features on the admin panel.	5.4	More Details
CVE-2023-4007	Cross-site Scripting (XSS) - Stored in GitHub repository thorsten/phpmyfaq prior to 3.1.16.	5.4	More Details
CVE-2023-38304	An issue was discovered in Webmin 2.021. A Stored Cross-Site Scripting (XSS) vulnerability was discovered in the Users and Groups functionality, allowing an attacker to store a malicious payload in the Group Name field when creating a new group.	5.4	More Details
CVE-2023-39151	Jenkins 2.415 and earlier, LTS 2.401.2 and earlier does not sanitize or properly encode URLs in build logs when transforming them into hyperlinks, resulting in a stored cross-site scripting (XSS) vulnerability exploitable by attackers able to control build log contents.	5.4	More Details
CVE-2023-39153	A cross-site request forgery (CSRF) vulnerability in Jenkins GitLab Authentication Plugin 1.17.1 and earlier allows attackers to trick users into logging in to the attacker's account.	5.4	More Details
CVE-2023-37692	An arbitrary file upload vulnerability in October CMS v3.4.4 allows attackers to execute arbitrary code via a crafted file.	5.4	More Details
CVE-2023-35792	Vound Intella Connect 2.6.0.3 is vulnerable to stored Cross-site Scripting (XSS).	5.4	More Details
CVE-2023-38303	An issue was discovered in Webmin 2.021. One can exploit a stored Cross-Site Scripting (XSS) attack to achieve Remote Command Execution (RCE) through the Users and Group's real name parameter.	5.4	More Details
CVE-2023-38331	Zoho ManageEngine Support Center Plus 14001 and below is vulnerable to stored XSS in the products module.	5.4	More Details
CVE-2023-36118	Cross Site Scripting vulnerability in Faculty Evaulation System using PHP/MySQLi v.1.0 allows an attacker to execute arbitrary code via a crafted payload to the page parameter.	5.4	More Details
CVE-2023-38307	An issue was discovered in Webmin 2.021. A Stored Cross-Site Scripting (XSS) vulnerability was discovered in the Users and Groups functionality. The vulnerability occurs when an authenticated user adds a new user and inserts an XSS payload into the user's real name.	5.4	More Details

CVE Number	Description	Base Score	Reference
CVE-2023-22595	IBM B2B Advanced Communications 1.0.0.0 and IBM Multi-Enterprise Integration Gateway 1.0.0.1 are vulnerable to cross-site scripting. This vulnerability allows users to embed arbitrary JavaScript code in the Web UI thus altering the intended functionality potentially leading to credentials disclosure within a trusted session. IBM X-Force ID: 244076.	5.4	More Details
CVE-2023-39156	A cross-site request forgery (CSRF) vulnerability in Jenkins Bazaar Plugin 1.22 and earlier allows attackers to delete previously created Bazaar SCM tags.	5.3	More Details
CVE-2023-38684	Discourse is an open source discussion platform. Prior to version 3.0.6 of the `stable` branch and version 3.1.0.beta7 of the `beta` and `tests-passed` branches, in multiple controller actions, Discourse accepts limit params but does not impose any upper bound on the values being accepted. Without an upper bound, the software may allow arbitrary users to generate DB queries which may end up exhausting the resources on the server. The issue is patched in version 3.0.6 of the `stable` branch and version 3.1.0.beta7 of the `beta` and `tests-passed` branches. There are no known workarounds for this vulnerability.	5.3	More Details
CVE-2023-38357	Session tokens in RWS WorldServer 11.7.3 and earlier have a low entropy and can be enumerated, leading to unauthorized access to user sessions.	5.3	More Details
CVE-2023-38492	Kirby is a content management system. A vulnerability in versions prior to 3.5.8.3, 3.6.6.3, 3.7.5.2, 3.8.4.1, and 3.9.6 affects all Kirby sites with user accounts (unless Kirby's API and Panel are disabled in the config). The real-world impact of this vulnerability is limited, however we still recommend to update to one of the patch releases because they also fix more severe vulnerabilities. Kirby's authentication endpoint did not limit the password length. This allowed attackers to provide a password with a length up to the server's maximum request body length. Validating that password against the user's actual password requires hashing the provided password, which requires more CPU and memory resources (and therefore processing time) the longer the provided password gets. This could be abused by an attacker to cause the website to become unresponsive or unavailable. Because Kirby comes with a built-in brute force protection, the impact of this vulnerability is limited to 10 failed logins from each IP address and 10 failed logins for each existing user per hour. The problem has been patched in Kirby 3.5.8.3, 3.6.6.3, 3.7.5.2, 3.8.4.1, and 3.9.6. In all of the mentioned releases, the maintainers have added password length limits in the affected code so that passwords longer than 1000 bytes are immediately blocked, both when setting a password and when logging in.	5.3	More Details

CVE Number	Description	Base Score	Reference
CVE-2023-4045	Offscreen Canvas did not properly track cross-origin tainting, which could have been used to access image data from another site in violation of same-origin policy. This vulnerability affects Firefox < 116, Firefox ESR < 102.14, and Firefox ESR < 115.1.	5.3	More Details
CVE-2023-39155	Jenkins Chef Identity Plugin 2.0.3 and earlier does not mask the user.pem key form field, increasing the potential for attackers to observe and capture it.	5.3	More Details
CVE-2023-3817	Issue summary: Checking excessively long DH keys or parameters may be very slow. Impact summary: Applications that use the functions DH_check(), DH_check_ex() or EVP_PKEY_param_check() to check a DH key or DH parameters may experience long delays. Where the key or parameters that are being checked have been obtained from an untrusted source this may lead to a Denial of Service. The function DH_check() performs various checks on DH parameters. After fixing CVE-2023-3446 it was discovered that a large q parameter value can also trigger an overly long computation during some of these checks. A correct q value, if present, cannot be larger than the modulus p parameter, thus it is unnecessary to perform these checks if q is larger than p. An application that calls DH_check() and supplies a key or parameters obtained from an untrusted source could be vulnerable to a Denial of Service attack. The function DH_check() is itself called by a number of other OpenSSL functions. An application calling any of those other functions may similarly be affected. The other functions affected by this are DH_check_ex() and EVP_PKEY_param_check(). Also vulnerable are the OpenSSL dhparam and pkeyparam command line applications when using the "-check" option. The OpenSSL SSL/TLS implementation is not affected by this issue. The OpenSSL 3.0 and 3.1 FIPS providers are not affected by this issue.	5.3	More Details
CVE-2023-3462	HashiCorp's Vault and Vault Enterprise are vulnerable to user enumeration when using the LDAP auth method. An attacker may submit requests of existent and non-existent LDAP users and observe the response from Vault to check if the account is valid on the LDAP server. This vulnerability is fixed in Vault 1.14.1 and 1.13.5.	5.3	More Details
CVE-2023-4046	In some circumstances, a stale value could have been used for a global variable in WASM JIT analysis. This resulted in incorrect compilation and a potentially exploitable crash in the content process. This vulnerability affects Firefox < 116, Firefox ESR < 102.14, and Firefox ESR < 115.1.	5.3	More Details
CVE-2023-37217	Tadiran Telecom Aeonix - CWE-204: Observable Response Discrepancy	5.3	More Details

CVE Number	Description	Base Score	Reference
CVE-2022-42182	Precisely Spectrum Spatial Analyst 20.01 is vulnerable to Directory Traversal.	5.3	More Details
CVE-2023-39261	In JetBrains IntelliJ IDEA before 2023.2 plugin for Space was requesting excessive permissions	5.2	More Details
CVE-2023-1401	An issue has been discovered in GitLab DAST scanner affecting all versions starting from 3.0.29 before 4.0.5, in which the DAST scanner leak cross site cookies on redirect during authorization.	5.0	More Details
CVE-2023-3774	An unhandled error in Vault Enterprise's namespace creation may cause the Vault process to crash, potentially resulting in denial of service. Fixed in 1.14.1, 1.13.5, and 1.12.9.	4.9	More Details
CVE-2023-3981	Server-Side Request Forgery (SSRF) in GitHub repository omeka/omeka-s prior to 4.0.2.	4.9	More Details
CVE-2023-31935	Cross Site Scripting vulnerability found in Rail Pass Management System v.1.0 allows a remote attacker to obtain sensitive information via the emial parameter of admin-profile.php.	4.8	More Details
CVE-2023-23764	An incorrect comparison vulnerability was identified in GitHub Enterprise Server that allowed commit smuggling by displaying an incorrect diff within the GitHub pull request UI. To do so, an attacker would need write access to the repository. This vulnerability affected GitHub Enterprise Server versions 3.7.0 and above and was fixed in versions 3.7.9, 3.8.2, and 3.9.1. This vulnerability was reported via the GitHub Bug Bounty program.	4.8	More Details
CVE-2023-31934	Cross Site Scripting vulnerability found in Rail Pass Management System v.1.0 allows a remote attacker to obtain sensitive information via the adminname parameter of admin-profile.php.	4.8	More Details
CVE-2021-31651	Cross Site Scripting (XSS) vulnerability in neofarg-cms 0.2.3 allows remoate attacker to run arbitrary code via the copyright field in copyright settings.	4.8	More Details
CVE-2023-3130	The Short URL WordPress plugin before 1.6.5 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-2023-3982	Cross-site Scripting (XSS) - Stored in GitHub repository omeka/omeka-s prior to 4.0.2.	4.8	More Details
CVE-2023-3980	Cross-site Scripting (XSS) - Stored in GitHub repository omeka/omeka-s prior to 4.0.2.	4.8	More Details
CVE-2023-37623	Netdisco before v2.063000 was discovered to contain a cross-site scripting (XSS) vulnerability via the component /Web/TypeAhead.pm.	4.8	More Details
CVE-2023-38670	Null pointer dereference in paddle.flip in PaddlePaddle before 2.5.0. This resulted in a runtime crash and denial of service.	4.7	More Details
CVE-2023-38672	FPE in paddle.trace in PaddlePaddle before 2.5.0. This flaw can cause a runtime crash and a denial of service.	4.7	More Details
CVE-2023-20583	A potential power side-channel vulnerability in AMD processors may allow an authenticated attacker to monitor the CPU power consumption as the data in a cache line changes over time potentially resulting in a leak of sensitive information.	4.7	More Details
CVE-2023-4010	A flaw was found in the USB Host Controller Driver framework in the Linux kernel. The usb_giveback_urb function has a logic loophole in its implementation. Due to the inappropriate judgment condition of the goto statement, the function cannot return under the input of a specific malformed descriptor file, so it falls into an endless loop, resulting in a denial of service.	4.6	More Details
CVE-2023-3733	Inappropriate implementation in WebApp Installs in Google Chrome prior to 115.0.5790.98 allowed a remote attacker to potentially spoof the contents of the Omnibox (URL bar) via a crafted HTML page. (Chromium security severity: Medium)	4.3	More Details
CVE-2023-3977	Several plugins for WordPress by Inisev are vulnerable to Cross-Site Request Forgery to unauthorized installation of plugins due to a missing nonce check on the handle_installation function that is called via the inisev_installation AJAX aciton in various versions. This makes it possible for unauthenticated attackers to install plugins from the limited list via a forged request granted they can trick a site administrator into performing an action such as clicking on a link.	4.3	More Details

CVE Number	Description	Base Score	Reference
CVE-2023-3734	Inappropriate implementation in Picture In Picture in Google Chrome prior to 115.0.5790.98 allowed a remote attacker to potentially spoof the contents of the Omnibox (URL bar) via a crafted HTML page. (Chromium security severity: Medium)	4.3	More Details
CVE-2023-3622	Access Control Bypass Vulnerability in the SolarWinds Platform that allows an underprivileged user to read arbitrary resource	4.3	More Details
CVE-2023-30949	A missing origin validation in Slate sandbox could be exploited by a malicious user to modify the page's content, which could lead to phishing attacks.	4.3	More Details
CVE-2023-3735	Inappropriate implementation in Web API Permission Prompts in Google Chrome prior to 115.0.5790.98 allowed a remote attacker to obfuscate security UI via a crafted HTML page. (Chromium security severity: Medium)	4.3	More Details
CVE-2023-3957	The ACF Photo Gallery Field plugin for WordPress is vulnerable to unauthorized modification of data due to an insufficient restriction on the 'apg_profile_update' function in versions up to, and including, 1.9. This makes it possible for authenticated attackers, with subscriber-level permissions or above, to update the user metas arbitrarily. The meta value can only be a string.	4.3	More Details
CVE-2023-3736	Inappropriate implementation in Custom Tabs in Google Chrome on Android prior to 115.0.5790.98 allowed a remote attacker to leak cross-origin data via a crafted HTML page. (Chromium security severity: Medium)	4.3	More Details
CVE-2023-3737	Inappropriate implementation in Notifications in Google Chrome prior to 115.0.5790.98 allowed a remote attacker to spoof the contents of media notifications via a crafted HTML page. (Chromium security severity: Medium)	4.3	More Details
CVE-2023-3738	Inappropriate implementation in Autofill in Google Chrome prior to 115.0.5790.98 allowed a remote attacker to obfuscate security UI via a crafted HTML page. (Chromium security severity: Medium)	4.3	More Details
CVE-2023-38989	An issue in the delete function in the UserController class of jeesite v1.2.6 allows authenticated attackers to arbitrarily delete the Administrator's role information.	4.3	More Details

CVE Number	Description	Base Score	Reference
CVE-2023-0958	Several plugins for WordPress by Inisev are vulnerable to unauthorized installation of plugins due to a missing capability check on the handle_installation function that is called via the inisev_installation AJAX aciton in various versions. This makes it possible for authenticated attackers with minimal permissions, such as subscribers, to install select plugins from Inisev on vulnerable sites. CVE-2023-38514 appears to be a duplicate of this vulnerability.	4.3	More Details
CVE-2023-3740	Insufficient validation of untrusted input in Themes in Google Chrome prior to 115.0.5790.98 allowed a remote attacker to potentially serve malicious content to a user via a crafted background URL. (Chromium security severity: Low)	4.3	More Details
CVE-2023-38685	Discourse is an open source discussion platform. Prior to version 3.0.6 of the `stable` branch and version 3.1.0.beta7 of the `beta` and `tests-passed` branches, information about restricted-visibility topic tags could be obtained by unauthorized users. The issue is patched in version 3.0.6 of the `stable` branch and version 3.1.0.beta7 of the `beta` and `tests-passed` branches.	4.3	More Details
CVE-2022-4908	Inappropriate implementation in iFrame Sandbox in Google Chrome prior to 107.0.5304.62 allowed a remote attacker to leak cross-origin data via a crafted HTML page. (Chromium security severity: Medium)	4.3	More Details
CVE-2021-4316	Inappropriate implementation in Cast UI in Google Chrome prior to 96.0.4664.45 allowed a remote attacker to spoof browser UI via a crafted HTML page. (Chromium security severity: Low)	4.3	More Details
CVE-2023-38988	An issue in the delete function in the OaNotifyController class of jeesite v1.2.6 allows authenticated attackers to arbitrarily delete notifications created by Administrators.	4.3	More Details
CVE-2023-38498	Discourse is an open source discussion platform. Prior to version 3.0.6 of the `stable` branch and version 3.1.0.beta7 of the `beta` and `tests-passed` branches, a malicious user can prevent the defer queue from proceeding promptly on sites hosted in the same multisite installation. The issue is patched in version 3.0.6 of the `stable` branch and version 3.1.0.beta7 of the `beta` and `tests-passed` branches. There are no known workarounds for this vulnerability. Users of multisite configurations should upgrade.	4.3	More Details
CVE-2022-4917	Incorrect security UI in Notifications in Google Chrome on Android prior to 103.0.5060.53 allowed a remote attacker to obscure the full screen notification via a crafted HTML page. (Chromium security severity: Low)	4.3	More Details

CVE Number	Description	Base Score	Reference
CVE-2023-37906	Discourse is an open source discussion platform. Prior to version 3.0.6 of the `stable` branch and version 3.1.0.beta7 of the `beta` and `tests-passed` branches, a malicious user can edit a post in a topic and cause a DoS with a carefully crafted edit reason. The issue is patched in version 3.0.6 of the `stable` branch and version 3.1.0.beta7 of the `beta` and `tests-passed` branches. There are no known workarounds for this vulnerability.	4.3	More Details
CVE-2020-4868	IBM TRIRIGA 3.0, 4.0, and 4.4 could allow a remote attacker to obtain sensitive information when a detailed technical error message is returned in the browser. This information could be used in further attacks against the system. IBM X-Force ID: 190744.	4.3	More Details
CVE-2021-4321	Policy bypass in Blink in Google Chrome prior to 91.0.4472.77 allowed a remote attacker to bypass content security policy via a crafted HTML page. (Chromium security severity: Low)	4.3	More Details
CVE-2023-3488	Uninitialized buffer in GBL parser in Silicon Labs GSDK v4.3.0 and earlier allows attacker to leak data from Secure stack via malformed GBL file.	3.8	More Details
CVE-2023-3947	The Video Conferencing with Zoom plugin for WordPress is vulnerable to Sensitive Information Exposure due to hardcoded encryption key on the 'vczapi_encrypt_decrypt' function in versions up to, and including, 4.2.1. This makes it possible for unauthenticated attackers to decrypt and view the meeting id and password.	3.7	More Details
CVE-2023-3970	A vulnerability, which was classified as problematic, was found in GZ Scripts Availability Booking Calendar PHP 1.0. This affects an unknown part of the file /index.php?controller=GzUser&action=edit&id=1 of the component Image Handler. The manipulation of the argument img leads to cross site scripting. It is possible to initiate the attack remotely. The exploit has been disclosed to the public and may be used. The identifier VDB-235569 was assigned to this vulnerability.	3.5	More Details
CVE-2023-3969	A vulnerability, which was classified as problematic, has been found in GZ Scripts Availability Booking Calendar PHP 1.0. Affected by this issue is some unknown functionality of the file index.php of the component HTTP POST Request Handler. The manipulation of the argument promo_code leads to cross site scripting. 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-235568.	3.5	More Details

CVE Number	Description	Base Score	Reference
CVE-2023-3989	A vulnerability was found in SourceCodester Jewelry Store System 1.0. It has been rated as problematic. Affected by this issue is some unknown functionality of the file add_customer.php. The manipulation leads to cross site scripting. The attack may be launched remotely. VDB-235610 is the identifier assigned to this vulnerability.	3.5	More Details
CVE-2023-33229	The SolarWinds Platform was susceptible to the Incorrect Input Neutralization Vulnerability. This vulnerability allows a remote adversary with a valid SolarWinds Platform account to append URL parameters to inject passive HTML.	3.5	More Details
CVE-2023-3990	A vulnerability classified as problematic has been found in Mingsoft MCMS up to 5.3.1. This affects an unknown part of the file search.do of the component HTTP POST Request Handler. The manipulation of the argument style leads to cross site scripting. It is possible to initiate the attack remotely. The exploit has been disclosed to the public and may be used. It is recommended to apply a patch to fix this issue. The associated identifier of this vulnerability is VDB-235611.	3.5	More Details
CVE-2023-37900	Crossplane is a framework for building cloud native control planes without needing to write code. In versions prior to 1.11.5, 1.12.3, and 1.13.0, a high-privileged user could create a Package referencing an arbitrarily large image containing that Crossplane would then parse, possibly resulting in exhausting all the available memory and therefore in the container being OOMKilled. The impact is limited due to the high privileges required to be able to create the Package and the eventually consistency nature of controller. This issue is fixed in versions 1.11.5, 1.12.3, and 1.13.0.	3.4	More Details
CVE-2022-4923	Inappropriate implementation in Omnibox in Google Chrome prior to 99.0.4844.51 allowed an attacker in a privileged network position to perform a man-in-the-middle attack via malicious network traffic. (Chromium security severity: Low)	3.1	More Details
CVE-2023-37904	Discourse is an open source discussion platform. Prior to version 3.0.6 of the `stable` branch and version 3.1.0.beta7 of the `beta` and `tests-passed` branches, more users than permitted could be created from invite links. The issue is patched in version 3.0.6 of the `stable` branch and version 3.1.0.beta7 of the `beta` and `tests-passed` branches. As a workaround, use restrict to email address invites.	2.6	More Details

CVE Number	Description	Base Score	Reference
CVE-2023-3986	A vulnerability was found in SourceCodester Simple Online Mens Salon Management System 1.0 and classified as problematic. This issue affects some unknown processing of the file /admin/?page=user/list. The manipulation of the argument First Name/Last Name/Username leads to cross site scripting. 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-235607.	2.4	More Details
CVE-2023-32001	Rejected reason: We issued this CVE pre-maturely, as we have subsequently realized that this issue points out a problem that there really is no safe measures around or protections for.	N/A	More Details
CVE-2023-3451	Rejected reason: Duplicate CVE. Please use CVE-2023-32297.	N/A	More Details
CVE-2023-29845	Rejected reason: DO NOT USE THIS CVE RECORD. ConsultIDs: none. Reason: This record was withdrawn by its CNA. Further investigation showed that it was not a security issue. Notes: none.	N/A	More Details
CVE-2023-4026	Rejected reason: ** REJECT ** DO NOT USE THIS CVE RECORD. ConsultIDs: CVE-2023-4024. Reason: This record is a duplicate of CVE-2023-4024. Notes: All CVE users should reference CVE-2023-4024 instead of this record. All references and descriptions in this record have been removed to prevent accidental usage.	N/A	More Details
CVE-2023-39190	Rejected reason: CVE-2023-39190 was found to be a duplicate of CVE-2023-31436. Please see https://access.redhat.com/security/cve/CVE-2023-31436 for information about affected products and security errata.	N/A	More Details
CVE-2023-32302	Rejected reason: Authoritative user requested CVE rejection https://github.com/github/advisory-database/pull/2575#issuecomment-1745811653	N/A	More Details