SingCERT
Singapore Cyber Emergency Response Team

Security Bulletin 28 December 2022

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

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

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

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

CRITICAL VULNERABILITIES

CVE Number	Description	Base Score	Reference
CVE-2021-4140	It was possible to construct specific XSLT markup that would be able to bypass an iframe sandbox. This vulnerability affects Firefox ESR < 91.5, Firefox < 96, and Thunderbird < 91.5.	10.0	More Details
CVE-2022-46642	D-Link DIR-846 A1_FW100A43 was discovered to contain a command injection vulnerability via the auto_upgrade_hour parameter in the SetAutoUpgradeInfo function.	9.9	More Details
CVE-2022-46641	D-Link DIR-846 A1_FW100A43 was discovered to contain a command injection vulnerability via the lan(0)_dhcps_staticlist parameter in the SetIpMacBindSettings function.	9.9	More Details
CVE-2022-25893	The package vm2 before 3.9.10 are vulnerable to Arbitrary Code Execution due to the usage of prototype lookup for the WeakMap.prototype.set method. Exploiting this vulnerability leads to access to a host object and a sandbox compromise.	9.8	More Details
CVE-2022-45718	IP-COM M50 V15.11.0.33(10768) was discovered to contain a buffer overflow via the rules parameter in the formIPMacBindAdd function.	9.8	More Details
CVE-2022-44640	Heimdal before 7.7.1 allows remote attackers to execute arbitrary code because of an invalid free in the ASN.1 codec used by the Key Distribution Center (KDC).	9.8	More Details
CVE-2022-44015	An issue was discovered in Simmeth Lieferantenmanager before 5.6. An attacker can inject raw SQL queries. By activating MSSQL features, the attacker is able to execute arbitrary commands on the MSSQL server via the xp_cmdshell extended procedure.	9.8	More Details
CVE-2022-47949	The Nintendo NetworkBuffer class, as used in Animal Crossing: New Horizons before 2.0.6 and other products, allows remote attackers to execute arbitrary code via a large UDP packet that causes a buffer overflow, aka ENLBufferPwn. The victim must join a game session with the attacker. Other affected products include Mario Kart 7 before 1.2, Mario Kart 8, Mario Kart 8 Deluxe before 2.1.0, ARMS before 5.4.1, Splatoon, Splatoon 2 before 5.5.1, Splatoon 3 before late 2022, Super Mario Maker 2 before 3.0.2, and Nintendo Switch Sports before late 2022.	9.8	More Details
CVE-2022-47945	ThinkPHP Framework before 6.0.14 allows local file inclusion via the lang parameter when the language pack feature is enabled (lang_switch_on=true). An unauthenticated and remote attacker can exploit this to execute arbitrary operating system commands, as demonstrated by including pearcmd.php.	9.8	More Details
CVE-2022-45721	IP-COM M50 V15.11.0.33(10768) was discovered to contain a buffer overflow via the picName parameter in the formDelWewifiPic function.	9.8	More Details

CVE Number	Description	Base Score	Reference
CVE-2022-45720	IP-COM M50 V15.11.0.33(10768) was discovered to contain multiple buffer overflows via the ip, mac, and remark parameters in the formIPMacBindModify function.	9.8	More Details
CVE-2022-45719	IP-COM M50 V15.11.0.33(10768) was discovered to contain a buffer overflow via the gotoUrl parameter in the formPortalAuth function.	9.8	More Details
CVE-2022-45717	IP-COM M50 V15.11.0.33(10768) was discovered to contain a command injection vulnerability via the usbPartitionName parameter in the formSetUSBPartitionUmount function. This vulnerability is exploited via a crafted GET request.	9.8	More Details
CVE-2021-45466	In CWP (aka Control Web Panel or CentOS Web Panel) before 0.9.8.1107, attackers can make a crafted request to api/?api=add_server&DHCP= to add an authorized_keys text file in the /resources/ folder.	9.8	More Details
CVE-2022-45716	IP-COM M50 V15.11.0.33(10768) was discovered to contain a buffer overflow via the indexSet parameter in the formIPMacBindDel function.	9.8	More Details
CVE-2022-45715	IP-COM M50 V15.11.0.33(10768) was discovered to contain multiple buffer overflows via the pLanPortRange and pWanPortRange parameters in the formSetPortMapping function.	9.8	More Details
CVE-2022-45714	IP-COM M50 V15.11.0.33(10768) was discovered to contain a buffer overflow via the indexSet parameter in the formQOSRuleDel function.	9.8	More Details
CVE-2022-45712	IP-COM M50 V15.11.0.33(10768) was discovered to contain a buffer overflow via the rules parameter in the formAddDnsForward function.	9.8	More Details
CVE-2022-47635	Wildix WMS 6 before 6.02.20221216, WMS 5 before 5.04.20221214, and WMS4 before 4.04.45396.23 allows Server-side request forgery (SSRF) via ZohoClient.php.	9.8	More Details
CVE-2022-45710	IP-COM M50 V15.11.0.33(10768) was discovered to contain multiple buffer overflows via the pEnable, pLevel, and pModule parameters in the formSetDebugCfg function.	9.8	More Details
CVE-2022-45896	Planet eStream before 6.72.10.07 allows unauthenticated upload of arbitrary files: Choose a Video / Related Media or Upload Document. Upload2.ashx can be used, or Ajax.asmx/ProcessUpload2. This leads to remote code execution.	9.8	More Details
CVE-2021-45467	In CWP (aka Control Web Panel or CentOS Web Panel) before 0.9.8.1107, an unauthenticated attacker can use %00 bytes to cause /user/loader.php to register an arbitrary API key, as demonstrated by a /user/loader.php?api=1&scripts= .%00./.%00./api/account_new_create&acc=guadaapi URI. Any number of %00 instances can be used, e.g., .%00%00%00./.%00%00%00./api/account_new_create could also be used for the scripts parameter.	9.8	More Details
CVE-2022-45708	IP-COM M50 V15.11.0.33(10768) was discovered to contain a buffer overflow via the sPortMapIndex parameter in the formDelPortMapping function.	9.8	More Details
CVE-2022-24116	Certain General Electric Renewable Energy products have inadequate encryption strength. This affects iNET and iNET II before 8.3.0.	9.8	More Details
CVE-2022-45963	h3c firewall <= 3.10 ESS6703 has a privilege bypass vulnerability.	9.8	More Details
CVE-2022-45778	https://www.hillstonenet.com.cn/ Hillstone Firewall SG-6000 <= 5.0.4.0 is vulnerable to Incorrect Access Control. There is a permission bypass vulnerability in the Hillstone WEB application firewall. An attacker can enter the background of the firewall with super administrator privileges through a configuration error in report.m.	9.8	More Details
CVE-2021-4236	Web Sockets do not execute any AuthenticateMethod methods which may be set, leading to a nil pointer dereference if the returned UserData pointer is assumed to be non-nil, or authentication bypass. This issue only affects WebSockets with an AuthenticateMethod hook. Request handlers that do not explicitly use WebSockets are not vulnerable.	9.8	More Details
CVE-2017-20146	Usage of the CORS handler may apply improper CORS headers, allowing the requester to explicitly control the value of the Access-Control-Allow-Origin header, which bypasses the expected behavior of the Same Origin Policy.	9.8	More Details
CVE-2014-125026	LZ4 bindings use a deprecated C API that is vulnerable to memory corruption, which could lead to arbitrary code execution if called with untrusted user input.	9.8	More Details

CVE Number	Description	Base Score	Reference
CVE-2022-4724	Improper Access Control in GitHub repository ikus060/rdiffweb prior to 2.5.5.	9.8	More Details
CVE-2022-4719	Business Logic Errors in GitHub repository ikus060/rdiffweb prior to 2.5.5.	9.8	More Details
CVE-2022-46764	A SQL injection issue in the web API in TrueConf Server 5.2.0.10225 allows remote unauthenticated attackers to execute arbitrary SQL commands, ultimately leading to remote code execution.	9.8	More Details
CVE-2020-24600	Shilpi CAPExWeb 1.1 allows SQL injection via a servlet/capexweb.cap_sendMail GET request.	9.8	More Details
CVE-2019-11851	The ACENet service in Sierra Wireless ALEOS before 4.4.9, 4.5.x through 4.9.x before 4.9.5, and 4.10.x through 4.13.x before 4.14.0 allows remote attackers to execute arbitrary code via a buffer overflow.	9.8	More Details
CVE-2020-11101	Sierra Wireless AirLink Mobility Manager (AMM) before 2.17 mishandles sessions and thus an unauthenticated attacker can obtain a login session with administrator privileges.	9.8	More Details
CVE-2022-4120	The Stop Spammers Security	Block Spam Users, Comments, Forms WordPress plugin before 2022.6 passes base64 encoded user input to the unserialize() PHP function when CAPTCHA are used as second challenge, which could lead to PHP Object injection if a plugin installed on the blog has a suitable gadget chain	9.8	More Details
CVE-2022-4117	The IWS WordPress plugin through 1.0 does not properly escape a parameter before using it in a SQL statement via an AJAX action available to unauthenticated users, leading to an unauthenticated SQL injection.	9.8	More Details
CVE-2022-4047	The Return Refund and Exchange For WooCommerce WordPress plugin before 4.0.9 does not validate attachment files to be uploaded via an AJAX action available to unauthenticated users, which could allow them to upload arbitrary files such as PHP and lead to RCE	9.8	More Details
CVE-2022-26969	In Directus before 9.7.0, the default settings of CORS_ORIGIN and CORS_ENABLED are true.	9.8	More Details
CVE-2022-24119	Certain General Electric Renewable Energy products have a hidden feature for unauthenticated remote access to the device configuration shell. This affects iNET and iNET II before 8.3.0.	9.8	More Details
CVE-2022-24117	Certain General Electric Renewable Energy products download firmware without an integrity check. This affects iNET and iNET II before 8.3.0, SD before 6.4.7, TD220X before 2.0.16, and TD220MAX before 1.2.6.	9.8	More Details
CVE-2022-45709	IP-COM M50 V15.11.0.33(10768) was discovered to contain multiple command injection vulnerabilities via the pEnable, pLevel, and pModule parameters in the formSetDebugCfg function.	9.8	More Details
CVE-2022-45711	IP-COM M50 V15.11.0.33(10768) was discovered to contain a command injection vulnerability via the hostname parameter in the formSetNetCheckTools function.	9.8	More Details
CVE-2022-45707	IP-COM M50 V15.11.0.33(10768) was discovered to contain a buffer overflow via the rules parameter in the formAddDnsHijack function.	9.8	More Details
CVE-2021-4129	Mozilla developers and community members Julian Hector, Randell Jesup, Gabriele Svelto, Tyson Smith, Christian Holler, and Masayuki Nakano reported memory safety bugs present in Firefox 94. 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 < 95, Firefox ESR < 91.4.0, and Thunderbird < 91.4.0.	9.8	More Details
CVE-2022-34470	Session history navigations may have led to a use-after-free and potentially exploitable crash. This vulnerability affects Firefox < 102, Firefox ESR < 91.11, Thunderbird < 102, and Thunderbird < 91.11.	9.8	More Details
CVE-2022-31748	Mozilla developers Gabriele Svelto, Timothy Nikkel, Randell Jesup, Jon Coppeard, and the Mozilla Fuzzing Team reported memory safety bugs present in Firefox 100. 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 < 101.	9.8	More Details
CVE-2022-45706	IP-COM M50 V15.11.0.33(10768) was discovered to contain a buffer overflow via the hostname parameter in the formSetNetCheckTools function.	9.8	More Details
CVE-2022-31737	A malicious webpage could have caused an out-of-bounds write in WebGL, leading to memory corruption and a potentially exploitable crash. This vulnerability affects Thunderbird < 91.10, Firefox < 101, and Firefox ESR < 91.10.	9.8	More Details

CVE Number	Description	Base Score	Reference
CVE-2022-31736	A malicious website could have learned the size of a cross-origin resource that supported Range requests. This vulnerability affects Thunderbird < 91.10, Firefox < 101, and Firefox ESR < 91.10.	9.8	More Details
CVE-2022-29917	Mozilla developers Andrew McCreight, Gabriele Svelto, Tom Ritter and the Mozilla Fuzzing Team reported memory safety bugs present in Firefox 99 and Firefox ESR 91.8. 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 Thunderbird < 91.9, Firefox ESR < 91.9, and Firefox < 100.	9.8	More Details
CVE-2022-1887	The search term could have been specified externally to trigger SQL injection. This vulnerability affects Firefox for iOS < 101.	9.8	More Details
CVE-2021-4127	An out of date graphics library (Angle) likely contained vulnerabilities that could potentially be exploited. This vulnerability affects Thunderbird < 78.9 and Firefox ESR < 78.9.	9.8	More Details
CVE-2022-34485	Mozilla developers Bryce Seager van Dyk and the Mozilla Fuzzing Team reported potential vulnerabilities present in Firefox 101. 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 < 102.	9.8	More Details
CVE-2022-47926	AyaCMS 3.1.2 is vulnerable to file deletion via /aya/module/admin/fst_del.inc.php	9.8	More Details
CVE-2022-46102	AyaCMS 3.1.2 is vulnerable to Arbitrary file upload via /aya/module/admin/fst_down.inc.php	9.8	More Details
CVE-2022-45966	here is an arbitrary file upload vulnerability in the file management function module of Classcms3.5.	9.8	More Details
CVE-2022-45347	Apache ShardingSphere-Proxy prior to 5.3.0 when using MySQL as database backend didn't cleanup the database session completely after client authentication failed, which allowed an attacker to execute normal commands by constructing a special MySQL client. This vulnerability has been fixed in Apache ShardingSphere 5.3.0.	9.8	More Details
CVE-2022-3184	Dataprobe iBoot-PDU FW versions prior to 1.42.06162022 contain a vulnerability where the device's existing firmware allows unauthenticated users to access an old PHP page vulnerable to directory traversal, which may allow a user to write a file to the webroot directory.	9.8	More Details
CVE-2022-3183	Dataprobe iBoot-PDU FW versions prior to 1.42.06162022 contain a vulnerability where a specific function does not sanitize the input provided by the user, which may expose the affected to an OS command injection vulnerability.	9.8	More Details
CVE-2022-40145	This vulnerable is about a potential code injection when an attacker has control of the target LDAP server using in the JDBC JNDI URL. The function jaas.modules.src.main.java.porg.apache.karaf.jass.modules.jdbc.JDBCUtils#doCreateDatasource use InitialContext.lookup(jndiName) without filtering. An user can modify `options.put(JDBCUtils.DATASOURCE, "osgi:" + DataSource.class.getName());` to `options.put(JDBCUtils.DATASOURCE,"jndi:rmi://x.x.x.x:xxxx/Command");` in JdbcLoginModuleTest#setup. This is vulnerable to a remote code execution (RCE) attack when a configuration uses a JNDI LDAP data source URI when an attacker has control of the target LDAP server.This issue affects all versions of Apache Karaf up to 4.4.1 and 4.3.7. We encourage the users to upgrade to Apache Karaf at least 4.4.2 or 4.3.8	9.8	More Details
CVE-2022-34476	ASN.1 parsing of an indefinite SEQUENCE inside an indefinite GROUP could have resulted in the parser accepting malformed ASN.1. This vulnerability affects Firefox < 102.	9.8	More Details
CVE-2022-31747	Mozilla developers Andrew McCreight, Nicolas B. Pierron, and the Mozilla Fuzzing Team reported memory safety bugs present in Firefox 100 and Firefox ESR 91.9. 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 Thunderbird < 91.10, Firefox < 101, and Firefox ESR < 91.10.	9.8	More Details
CVE-2022-36320	Mozilla developers and the Mozilla Fuzzing Team reported memory safety bugs present in Firefox 102. 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 < 103.	9.8	More Details
CVE-2022-41794	A heap based buffer overflow vulnerability exists in the PSD thumbnail resource parsing code of OpenImageIO 2.3.19.0. A specially-crafted PSD file can lead to arbitrary code execution. An attacker can provide a malicious file to trigger this vulnerability.	9.8	More Details

CVE Number	Description	Base Score	Reference
CVE-2022-47939	An issue was discovered in ksmbd in the Linux kernel 5.15 through 5.19 before 5.19.2. fs/ksmbd/smb2pdu.c has a use-after-free and OOPS for SMB2_TREE_DISCONNECT.	9.8	More Details
CVE-2022-44567	A command injection vulnerability exists in Rocket.Chat-Desktop <3.8.14 that could allow an attacker to pass a malicious url of openInternalVideoChatWindow to shell.openExternal(), which may lead to remote code execution (internalVideoChatWindow.ts#L17). To exploit the vulnerability, the internal video chat window must be disabled or a Mac App Store build must be used (internalVideoChatWindow.ts#L14). The vulnerability may be exploited by an XSS attack because the function openInternalVideoChatWindow is exposed in the Rocket.Chat-Desktop-API.	9.8	More Details
CVE-2022-4686	Authorization Bypass Through User-Controlled Key in GitHub repository usememos/memos prior to 0.9.0.	9.8	More Details
CVE-2022-46493	Default version of nbnbk was discovered to contain an arbitrary file upload vulnerability via the component /api/User/download_img.	9.8	More Details
CVE-2022-41838	A code execution vulnerability exists in the DDS scanline parsing functionality of OpenImageIO Project OpenImageIO v2.4.4.2. A specially-crafted .dds can lead to a heap buffer overflow. An attacker can provide a malicious file to trigger this vulnerability.	9.8	More Details
CVE-2022-45406	If an out-of-memory condition occurred when creating a JavaScript global, a JavaScript realm may be deleted while references to it lived on in a BaseShape. This could lead to a use-after-free causing a potentially exploitable crash. This vulnerability affects Firefox ESR < 102.5, Thunderbird < 102.5, and Firefox < 107.	9.8	More Details
CVE-2022-41837	An out-of-bounds write vulnerability exists in the OpenImageIO::add_exif_item_to_spec functionality of OpenImageIO Project OpenImageIO v2.4.4.2. Specially-crafted exif metadata can lead to stack-based memory corruption. An attacker can provide a malicious file to trigger this vulnerability.	9.8	More Details
CVE-2022-46442	dedecms <=V5.7.102 is vulnerable to SQL Injection. In sys_ sql_ n query.php there are no restrictions on the sql query.	9.8	More Details
CVE-2022-46882	A use-after-free in WebGL extensions could have led to a potentially exploitable crash. This vulnerability affects Firefox < 107, Firefox ESR < 102.6, and Thunderbird < 102.6.	9.8	More Details
CVE-2022-41639	A heap based buffer overflow vulnerability exists in tile decoding code of TIFF image parser in OpenImageIO master-branch-9aeece7a and v2.3.19.0. A specially-crafted TIFF file can lead to an out of bounds memory corruption, which can result in arbitrary code execution. An attacker can provide a malicious file to trigger this vulnerability.	9.8	More Details
CVE-2022-38143	A heap out-of-bounds write vulnerability exists in the way OpenImageIO v2.3.19.0 processes RLE encoded BMP images. A specially-crafted bmp file can write to arbitrary out of bounds memory, which can lead to arbitrary code execution. An attacker can provide a malicious file to trigger this vulnerability.	9.8	More Details
CVE-2021-32692	Activity Watch is a free and open-source automated time tracker. Versions prior to 0.11.0 allow an attacker to execute arbitrary commands on any macOS machine with ActivityWatch running. The attacker can exploit this vulnerability by having the user visiting a website with the page title set to a malicious string. An attacker could use another application to accomplish the same, but the web browser is the most likely attack vector. This issue is patched in version 0.11.0. As a workaround, users can run the latest version of aw-watcher-window from source, or manually patch the `printAppTitle.scpt` file.	9.6	More Details
CVE-2022-26384	If an attacker could control the contents of an iframe sandboxed with <code>allow-popups</code> but not <code>allow-scripts</code>, they were able to craft a link that, when clicked, would lead to JavaScript execution in violation of the sandbox. This vulnerability affects Firefox < 98, Firefox ESR < 91.7, and Thunderbird < 91.7.	9.6	More Details
CVE-2022-26486	An unexpected message in the WebGPU IPC framework could lead to a use-after-free and exploitable sandbox escape. We have had reports of attacks in the wild abusing this flaw. This vulnerability affects Firefox < 97.0.2, Firefox ESR < 91.6.1, Firefox for Android < 97.3.0, Thunderbird < 91.6.2, and Focus < 97.3.0.	9.6	More Details
CVE-2022-22759	If a document created a sandboxed iframe without <code>allow-scripts</code>, and subsequently appended an element to the iframe's document that e.g. had a JavaScript event handler - the event handler would have run despite the iframe's sandbox. This vulnerability affects Firefox < 97, Thunderbird < 91.6, and Firefox ESR < 91.6.	9.6	More Details

CVE Number	Description	Base Score	Reference
CVE-2022-24118	Certain General Electric Renewable Energy products allow attackers to use a code to trigger a reboot into the factory default configuration. This affects iNET and iNET II before 8.3.0, SD before 6.4.7, TD220X before 2.0.16, and TD220MAX before 1.2.6.	9.1	More Details
CVE-2022-47931	IO FinNet tss-lib before 2.0.0 allows a collision of hash values.	9.1	More Details
CVE-2022-28228	Out-of-bounds read was discovered in YDB server. An attacker could construct a query with insert statement that would allow him to read sensitive information from other memory locations or cause a crash.	9.1	More Details
CVE-2022-41649	A heap out of bounds read vulnerability exists in the handling of IPTC data while parsing TIFF images in OpenImageIO v2.3.19.0. A specially-crafted TIFF file can cause a read of adjacent heap memory, which can leak sensitive process information. An attacker can provide a malicious file to trigger this vulnerability.	9.1	More Details
CVE-2020-36560	Due to improper path sanitization, archives containing relative file paths can cause files to be written (or overwritten) outside of the target directory.	9.1	More Details
CVE-2020-36561	Due to improper path sanitization, archives containing relative file paths can cause files to be written (or overwritten) outside of the target directory.	9.1	More Details
CVE-2020-36566	Due to improper path sanitization, archives containing relative file paths can cause files to be written (or overwritten) outside of the target directory.	9.1	More Details
CVE-2020-36569	Authentication is globally bypassed in github.com/nanobox-io/golang-nanoauth between v0.0.0-20160722212129-ac0cc4484ad4 and v0.0.0-20200131131040-063a3fb69896 if ListenAndServe is called with an empty token.	9.1	More Details
CVE-2021-4238	Randomly-generated alphanumeric strings contain significantly less entropy than expected. The RandomAlphaNumeric and CryptoRandomAlphaNumeric functions always return strings containing at least one digit from 0 to 9. This significantly reduces the amount of entropy in short strings generated by these functions.	9.1	More Details
CVE-2022-45891	Planet eStream before 6.72.10.07 allows attackers to call restricted functions, and perform unauthenticated uploads (Upload2.ashx) or access content uploaded by other users (View.aspx after Ajax.asmx/SaveGrantAccessList).	9.1	More Details
CVE-2022-44013	An issue was discovered in Simmeth Lieferantenmanager before 5.6. An attacker can make various API calls without authentication because the password in a Credential Object is not checked.	9.1	More Details
CVE-2018-25046	Due to improper path sanitization, archives containing relative file paths can cause files to be written (or overwritten) outside of the target directory.	9.1	More Details

OTHER VULNERABILITIES

CVE Number	Description	Base Score	Reference
CVE-2022-46873	Because Firefox did not implement the <code>unsafe-hashes</code> CSP directive, an attacker who was able to inject markup into a page otherwise protected by a Content Security Policy may have been able to inject executable script. This would be severely constrained by the specified Content Security Policy of the document. This vulnerability affects Firefox < 108.	8.8	More Details
CVE-2022-34484	The Mozilla Fuzzing Team reported potential vulnerabilities present in Thunderbird 91.10. 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 < 102, Firefox ESR < 91.11, Thunderbird < 102, and Thunderbird < 91.11.	8.8	More Details
CVE-2022-38473	A cross-origin iframe referencing an XSLT document would inherit the parent domain's permissions (such as microphone or camera access). This vulnerability affects Thunderbird < 102.2, Thunderbird < 91.13, Firefox ESR < 91.13, Firefox ESR < 102.2, and Firefox < 104.	8.8	More Details
CVE-2022-22738	Applying a CSS filter effect could have accessed out of bounds memory. This could have lead to a heap-buffer-overflow causing a potentially exploitable crash. This vulnerability affects Firefox ESR < 91.5, Firefox < 96, and Thunderbird < 91.5.	8.8	More Details

CVE Number	Description	Base Score	Reference
CVE-2022-38477	Mozilla developer Nika Layzell and the Mozilla Fuzzing Team reported memory safety bugs present in Firefox 103 and Firefox ESR 102.1. 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 ESR < 102.2, Thunderbird < 102.2, and Firefox < 104.	8.8	More Details
CVE-2022-38478	Members the Mozilla Fuzzing Team reported memory safety bugs present in Firefox 103, Firefox ESR 102.1, and Firefox ESR 91.12. Some of these bugs showed evidence of memory corruption and we presume that with enough effort some of these could have been exploited to run arbitrary code. This vulnerability affects Thunderbird < 102.2, Thunderbird < 91.13, Firefox ESR < 91.13, Firefox ESR < 102.2, and Firefox < 104.	8.8	More Details
CVE-2022-1802	If an attacker was able to corrupt the methods of an Array object in JavaScript via prototype pollution, they could have achieved execution of attacker-controlled JavaScript code in a privileged context. This vulnerability affects Firefox ESR < 91.9.1, Firefox < 100.0.2, Firefox for Android < 100.3.0, and Thunderbird < 91.9.1.	8.8	More Details
CVE-2022-1529	An attacker could have sent a message to the parent process where the contents were used to double-index into a JavaScript object, leading to prototype pollution and ultimately attacker-controlled JavaScript executing in the privileged parent process. This vulnerability affects Firefox ESR < 91.9.1, Firefox < 100.0.2, Firefox for Android < 100.3.0, and Thunderbird < 91.9.1.	8.8	More Details
CVE-2022-40962	Mozilla developers Nika Layzell, Timothy Nikkel, Sebastian Hengst, Andreas Pehrson, and the Mozilla Fuzzing Team reported memory safety bugs present in Firefox 104 and Firefox ESR 102.2. 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 ESR < 102.3, Thunderbird < 102.3, and Firefox < 105.	8.8	More Details
CVE-2022-0843	Mozilla developers Kershaw Chang, Ryan VanderMeulen, and Randell Jesup reported memory safety bugs present in Firefox 97. 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 < 98.	8.8	More Details
CVE-2022-0566	It may be possible for an attacker to craft an email message that causes Thunderbird to perform an out-of-bounds write of one byte when processing the message. This vulnerability affects Thunderbird < 91.6.1.	8.8	More Details
CVE-2022-0511	Mozilla developers and community members Gabriele Svelto, Sebastian Hengst, Randell Jesup, Luan Herrera, Lars T Hansen, and the Mozilla Fuzzing Team reported memory safety bugs present in Firefox 96. 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 < 97.	8.8	More Details
CVE-2022-42928	Certain types of allocations were missing annotations that, if the Garbage Collector was in a specific state, could have lead to memory corruption and a potentially exploitable crash. This vulnerability affects Firefox < 106, Firefox ESR < 102.4, and Thunderbird < 102.4.	8.8	More Details
CVE-2020-15685	During the plaintext phase of the STARTTLS connection setup, protocol commands could have been injected and evaluated within the encrypted session. This vulnerability affects Thunderbird < 78.7.	8.8	More Details
CVE-2022-42932	Mozilla developers Ashley Hale and the Mozilla Fuzzing Team reported memory safety bugs present in Firefox 105 and Firefox ESR 102.3. 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 < 106, Firefox ESR < 102.4, and Thunderbird < 102.4.	8.8	More Details
CVE-2022-46101	AyaCMS v3.1.2 was found to have a code flaw in the ust_sql.inc.php file, which allows attackers to cause command execution by inserting malicious code.	8.8	More Details
CVE-2022-45409	The garbage collector could have been aborted in several states and zones and <code>GCRuntime::finishCollection</code> may not have been called, leading to a use-after-free and potentially exploitable crash. This vulnerability affects Firefox ESR < 102.5, Thunderbird < 102.5, and Firefox < 107.	8.8	More Details
CVE-2022-45412	When resolving a symlink such as <code>file:///proc/self/fd/1</code>, an error message may be produced where the symlink was resolved to a string containing unitialized memory in the buffer. *This bug only affects Thunderbird on Unix-based operated systems (Android, Linux, MacOS). Windows is unaffected.*. This vulnerability affects Firefox ESR < 102.5, Thunderbird < 102.5, and Firefox < 107.	8.8	More Details

CVE Number	Description	Base Score	Reference
CVE-2022-45421	Mozilla developers Andrew McCreight and Gabriele Svelto reported memory safety bugs present in Thunderbird 102.4. 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 ESR < 102.5, Thunderbird < 102.5, and Firefox < 107.	8.8	More Details
CVE-2022-46871	An out of date library (libusrsctp) contained vulnerabilities that could potentially be exploited. This vulnerability affects Firefox < 108.	8.8	More Details
CVE-2022-28284	SVG's <code><use></code> element could have been used to load unexpected content that could have executed script in certain circumstances. While the specification seems to allow this, other browsers do not, and web developers relied on this property for script security so gecko's implementation was aligned with theirs. This vulnerability affects Firefox < 99.	8.8	More Details
CVE-2022-46874	A file with a long filename could have had its filename truncated to remove the valid extension, leaving a malicious extension in its place. This could potentially led to user confusion and the execution of malicious code. *Note*: This issue was originally included in the advisories for Thunderbird 102.6, but a patch (specific to Thunderbird) was omitted, resulting in it actually being fixed in Thunderbird 102.6.1. This vulnerability affects Firefox < 108, Thunderbird < 102.6.1, Thunderbird < 102.6, and Firefox ESR < 102.6.	8.8	More Details
CVE-2022-46878	Mozilla developers Randell Jesup, Valentin Gosu, Olli Pettay, and the Mozilla Fuzzing Team reported memory safety bugs present in Thunderbird 102.5. 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 < 108, Firefox ESR < 102.6, and Thunderbird < 102.6.	8.8	More Details
CVE-2022-46879	Mozilla developers and community members Lukas Bernhard, Gabriele Svelto, Randell Jesup, and the Mozilla Fuzzing Team reported memory safety bugs present in Firefox 107. 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 < 108.	8.8	More Details
CVE-2022-46881	An optimization in WebGL was incorrect in some cases, and could have led to memory corruption and a potentially exploitable crash. *Note*: This advisory was added on December 13th, 2022 after we better understood the impact of the issue. The fix was included in the original release of Firefox 106. This vulnerability affects Firefox < 106, Firefox ESR < 102.6, and Thunderbird < 102.6.	8.8	More Details
CVE-2022-22740	Certain network request objects were freed too early when releasing a network request handle. This could have lead to a use-after-free causing a potentially exploitable crash. This vulnerability affects Firefox ESR < 91.5, Firefox < 96, and Thunderbird < 91.5.	8.8	More Details
CVE-2022-22744	The constructed curl command from the "Copy as curl" feature in DevTools was not properly escaped for PowerShell. This could have lead to command injection if pasted into a Powershell prompt. *This bug only affects Thunderbird for Windows. Other operating systems are unaffected.*. This vulnerability affects Firefox ESR < 91.5, Firefox < 96, and Thunderbird < 91.5.	8.8	More Details
CVE-2022-46885	Mozilla developers Timothy Nikkel, Ashley Hale, and the Mozilla Fuzzing Team reported memory safety bugs present in Firefox 105. 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 < 106.	8.8	More Details
CVE-2022-34483	An attacker who could have convinced a user to drag and drop an image to a filesystem could have manipulated the resulting filename to contain an executable extension, and by extension potentially tricked the user into executing malicious code. While very similar, this is a separate issue from CVE-2022-34482. This vulnerability affects Firefox < 102.	8.8	More Details
CVE-2022-26485	Removing an XSLT parameter during processing could have lead to an exploitable use-after-free. We have had reports of attacks in the wild abusing this flaw. This vulnerability affects Firefox < 97.0.2, Firefox ESR < 91.6.1, Firefox for Android < 97.3.0, Thunderbird < 91.6.2, and Focus < 97.3.0.	8.8	More Details
CVE-2022-28288	Mozilla developers and community members Randell Jesup, Sebastian Hengst, and the Mozilla Fuzzing Team reported memory safety bugs present in Firefox 98. 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 < 99.	8.8	More Details

CVE Number	Description	Base Score	Reference
CVE-2022-28289	Mozilla developers and community members Nika Layzell, Andrew McCreight, Gabriele Svelto, and the Mozilla Fuzzing Team reported memory safety bugs present in Thunderbird 91.7. 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 Thunderbird < 91.8, Firefox < 99, and Firefox ESR < 91.8.	8.8	More Details
CVE-2022-29909	Documents in deeply-nested cross-origin browsing contexts could have obtained permissions granted to the top-level origin, bypassing the existing prompt and wrongfully inheriting the top-level permissions. This vulnerability affects Thunderbird < 91.9, Firefox ESR < 91.9, and Firefox < 100.	8.8	More Details
CVE-2022-29918	Mozilla developers Gabriele Svelto, Randell Jesup and the Mozilla Fuzzing Team reported memory safety bugs present in Firefox 99. 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 < 100.	8.8	More Details
CVE-2022-2200	If an object prototype was corrupted by an attacker, they would have been able to set undesired attributes on a JavaScript object, leading to privileged code execution. This vulnerability affects Firefox < 102, Firefox ESR < 91.11, Thunderbird < 102, and Thunderbird < 91.11.	8.8	More Details
CVE-2022-26381	An attacker could have caused a use-after-free by forcing a text reflow in an SVG object leading to a potentially exploitable crash. This vulnerability affects Firefox < 98, Firefox ESR < 91.7, and Thunderbird < 91.7.	8.8	More Details
CVE-2022-22764	Mozilla developers Paul Adenot and the Mozilla Fuzzing Team reported memory safety bugs present in Firefox 96 and Firefox ESR 91.5. 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 < 97, Thunderbird < 91.6, and Firefox ESR < 91.6.	8.8	More Details
CVE-2022-22763	When a worker is shutdown, it was possible to cause script to run late in the lifecycle, at a point after where it should not be possible. This vulnerability affects Firefox < 96, Thunderbird < 91.6, and Firefox ESR < 91.6.	8.8	More Details
CVE-2022-2505	Mozilla developers and the Mozilla Fuzzing Team reported memory safety bugs present in Firefox 102. 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 ESR < 102.1, Firefox < 103, and Thunderbird < 102.1.	8.8	More Details
CVE-2022-22761	Web-accessible extension pages (pages with a moz-extension:// scheme) were not correctly enforcing the frame-ancestors directive when it was used in the Web Extension's Content Security Policy. This vulnerability affects Firefox < 97, Thunderbird < 91.6, and Firefox ESR < 91.6.	8.8	More Details
CVE-2022-31739	When downloading files on Windows, the % character was not escaped, which could have lead to a download incorrectly being saved to attacker-influenced paths that used variables such as %HOMEPATH% or %APPDATA%. *This bug only affects Firefox for Windows. Other operating systems are unaffected.*. This vulnerability affects Thunderbird < 91.10, Firefox < 101, and Firefox ESR < 91.10.	8.8	More Details
CVE-2022-22758	When clicking on a tel: link, USSD codes, specified after a <code>*</code> character, would be included in the phone number. On certain phones, or on certain carriers, if the number was dialed this could perform actions on a user's account, similar to a cross-site request forgery attack. *This bug only affects Firefox for Android. Other operating systems are unaffected.*. This vulnerability affects Firefox < 97.	8.8	More Details
CVE-2022-31740	On arm64, WASM code could have resulted in incorrect assembly generation leading to a register allocation problem, and a potentially exploitable crash. This vulnerability affects Thunderbird < 91.10, Firefox < 101, and Firefox ESR < 91.10.	8.8	More Details
CVE-2022-22756	If a user was convinced to drag and drop an image to their desktop or other folder, the resulting object could have been changed into an executable script which would have run arbitrary code after the user clicked on it. This vulnerability affects Firefox < 97, Thunderbird < 91.6, and Firefox ESR < 91.6.	8.8	More Details
CVE-2022-22755	By using XSL Transforms, a malicious webserver could have served a user an XSL document that would continue to execute JavaScript (within the bounds of the same-origin policy) even after the tab was closed. This vulnerability affects Firefox < 97.	8.8	More Details
CVE-2022-31741	A crafted CMS message could have been processed incorrectly, leading to an invalid memory read, and potentially further memory corruption. This vulnerability affects Thunderbird < 91.10, Firefox < 101, and Firefox ESR < 91.10.	8.8	More Details

CVE Number	Description	Base Score	Reference
CVE-2022-34468	An iframe that was not permitted to run scripts could do so if the user clicked on a <code>javascript:</code> link. This vulnerability affects Firefox < 102, Firefox ESR < 91.11, Thunderbird < 102, and Thunderbird < 91.11.	8.8	More Details
CVE-2022-22752	Mozilla developers Christian Holler and Jason Kratzer reported memory safety bugs present in Firefox 95. 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 < 96.	8.8	More Details
CVE-2022-22751	Mozilla developers Calixte Denizet, Kershaw Chang, Christian Holler, Jason Kratzer, Gabriele Svelto, Tyson Smith, Simon Giesecke, and Steve Fink reported memory safety bugs present in Firefox 95 and Firefox ESR 91.4. 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 ESR < 91.5, Firefox < 96, and Thunderbird < 91.5.	8.8	More Details
CVE-2022-34480	Within the <code>lg_init()</code> function, if several allocations succeed but then one fails, an uninitialized pointer would have been freed despite never being allocated. This vulnerability affects Firefox < 102.	8.8	More Details
CVE-2022-34481	In the <code>nsTArray_Impl::ReplaceElementsAt()</code> function, an integer overflow could have occurred when the number of elements to replace was too large for the container. This vulnerability affects Firefox < 102, Firefox ESR < 91.11, Thunderbird < 102, and Thunderbird < 91.11.	8.8	More Details
CVE-2022-34482	An attacker who could have convinced a user to drag and drop an image to a filesystem could have manipulated the resulting filename to contain an executable extension, and by extension potentially tricked the user into executing malicious code. While very similar, this is a separate issue from CVE-2022-34483. This vulnerability affects Firefox < 102.	8.8	More Details
CVE-2022-46883	Mozilla developers Gabriele Svelto, Yulia Startsev, Andrew McCreight and the Mozilla Fuzzing Team reported memory safety bugs present in Firefox 106. 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. *Note*: This advisory was added on December 13th, 2022 after discovering it was inadvertently left out of the original advisory. The fix was included in the original release of Firefox 107. This vulnerability affects Firefox < 107.	8.8	More Details
CVE-2022-28281	If a compromised content process sent an unexpected number of WebAuthN Extensions in a Register command to the parent process, an out of bounds write would have occurred leading to memory corruption and a potentially exploitable crash. This vulnerability affects Thunderbird < 91.8, Firefox < 99, and Firefox ESR < 91.8.	8.8	More Details
CVE-2022-42898	PAC parsing in MIT Kerberos 5 (aka krb5) before 1.19.4 and 1.20.x before 1.20.1 has integer overflows that may lead to remote code execution (in KDC, kadmind, or a GSS or Kerberos application server) on 32-bit platforms (which have a resultant heap-based buffer overflow), and cause a denial of service on other platforms. This occurs in krb5_pac_parse in lib/krb5/krb/pac.c. Heimdal before 7.7.1 has "a similar bug."	8.8	More Details
CVE-2022-46763	A SQL injection issue in a database stored function in TrueConf Server 5.2.0.10225 allows a low-privileged database user to execute arbitrary SQL commands as the database administrator, resulting in execution of arbitrary code.	8.8	More Details
CVE-2022-40005	Intelbras WiFiber 120AC inMesh before 1-1-220826 allows command injection by authenticated users, as demonstrated by the /boaform/formPing6 and /boaform/formTracert URIs for ping and traceroute.	8.8	More Details
CVE-2022-4665	Unrestricted Upload of File with Dangerous Type in GitHub repository ampache/ampache prior to 5.5.6.	8.8	More Details
CVE-2022-4684	Improper Access Control in GitHub repository usememos/memos prior to 0.9.0.	8.8	More Details
CVE-2022-45893	Planet eStream before 6.72.10.07 allows a low-privileged user to gain access to administrative and high-privileged user accounts by changing the value of the ON cookie. A brute-force attack can calculate a value that provides permanent access.	8.8	More Details
CVE-2016-15005	CSRF tokens are generated using math/rand, which is not a cryptographically secure random number generator, allowing an attacker to predict values and bypass CSRF protections with relatively few requests.	8.8	More Details

CVE Number	Description	Base Score	Reference
CVE-2022-4689	Improper Access Control in GitHub repository usememos/memos prior to 0.9.0.	8.8	More Details
CVE-2022-4287	Authentication bypass in local application lock feature in Devolutions Remote Desktop Manager 2022.3.26 and earlier on Windows allows malicious user to access the application.	8.8	More Details
CVE-2022-4688	Improper Authorization in GitHub repository usememos/memos prior to 0.9.0.	8.8	More Details
CVE-2022-38065	A privilege escalation vulnerability exists in the oslo.privsep functionality of OpenStack git master 05194e7618 and prior. Overly permissive functionality within tools leveraging this library within a container can lead increased privileges.	8.8	More Details
CVE-2020-28191	The console in Togglz before 2.9.4 allows CSRF.	8.8	More Details
CVE-2022-47942	An issue was discovered in ksmbd in the Linux kernel 5.15 through 5.19 before 5.19.2. There is a heap-based buffer overflow in set_ntacl_dacl, related to use of SMB2_QUERY_INFO_HE after a malformed SMB2_SET_INFO_HE command.	8.8	More Details
CVE-2022-41318	A buffer over-read was discovered in libntlmauth in Squid 2.5 through 5.6. Due to incorrect integer-overflow protection, the SSPI and SMB authentication helpers are vulnerable to reading unintended memory locations. In some configurations, cleartext credentials from these locations are sent to a client. This is fixed in 5.7.	8.6	More Details
CVE-2022-46872	An attacker who compromised a content process could have partially escaped the sandbox to read arbitrary files via clipboard-related IPC messages. *This bug only affects Thunderbird for Linux. Other operating systems are unaffected.*. This vulnerability affects Firefox < 108, Firefox ESR < 102.6, and Thunderbird < 102.6.	8.6	More Details
CVE-2022-3805	The Jeg Elementor Kit plugin for WordPress is vulnerable to authorization bypass in various functions used to update the plugin settings in versions up to, and including, 2.5.6. Unauthenticated users can use an easily available nonce, obtained from pages edited by the plugin, to update the MailChimp API key, global styles, 404 page settings, and enabled elements.	8.6	More Details
CVE-2022-46170	CodeIgniter is a PHP full-stack web framework. When an application uses (1) multiple session cookies (e.g., one for user pages and one for admin pages) and (2) a session handler is set to `DatabaseHandler`, `MemcachedHandler`, or `RedisHandler`, then if an attacker gets one session cookie (e.g., one for user pages), they may be able to access pages that require another session cookie (e.g., for admin pages). This issue has been patched, please upgrade to version 4.2.11 or later. As a workaround, use only one session cookie.	8.6	More Details
CVE-2022-3186	Dataprobe iBoot-PDU FW versions prior to 1.42.06162022 contain a vulnerability where the affected product allows an attacker to access the device’s main management page from the cloud. This feature enables users to remotely connect devices, however, the current implementation permits users to access other device's information.	8.6	More Details
CVE-2022-36222	Nokia Fastmile 3tg00118abad52 devices shipped by Optus are shipped with a default hardcoded admin account of admin:Nq+L5st7o This account can be used locally to access the web admin interface.	8.4	More Details
CVE-2022-41290	IBM AIX 7.1, 7.2, 7.3, and VIOS 3.1 could allow a non-privileged local user to exploit a vulnerability in the rm_rlcache_file command to obtain root privileges. IBM X-Force ID: 236690.	8.4	More Details
CVE-2021-35954	fastrack Reflex 2.0 W307S_REFLEX_v90.89 Activity Tracker allows physically proximate attackers to dump the firmware, flash custom malicious firmware, and brick the device via the Serial Wire Debug (SWD) feature.	8.1	More Details
CVE-2022-43602	Multiple code execution vulnerabilities exist in the IFFOutput::close() functionality of OpenImageIO Project OpenImageIO v2.4.4.2. A specially crafted ImageOutput Object can lead to a heap buffer overflow. An attacker can provide malicious input to trigger these vulnerabilities.This vulnerability arises when the `ymax` variable is set to 0xFFFF and `m_spec.format` is `TypeDesc::UINT8`	8.1	More Details

CVE Number	Description	Base Score	Reference
CVE-2022-47633	An image signature validation bypass vulnerability in Kyverno 1.8.3 and 1.8.4 allows a malicious image registry (or a man-in-the-middle attacker) to inject unsigned arbitrary container images into a protected Kubernetes cluster. This is fixed in 1.8.5. This has been fixed in 1.8.5 and mitigations are available for impacted releases.	8.1	More Details
CVE-2022-47940	An issue was discovered in ksmbd in the Linux kernel 5.15 through 5.18 before 5.18.18. fs/ksmbd/smb2pdu.c lacks length validation in the non-padding case in smb2_write.	8.1	More Details
CVE-2022-3033	If a Thunderbird user replied to a crafted HTML email containing a <code>meta</code> tag, with the <code>meta</code> tag having the <code>http-equiv="refresh"</code> attribute, and the content attribute specifying an URL, then Thunderbird started a network request to that URL, regardless of the configuration to block remote content. In combination with certain other HTML elements and attributes in the email, it was possible to execute JavaScript code included in the message in the context of the message compose document. The JavaScript code was able to perform actions including, but probably not limited to, read and modify the contents of the message compose document, including the quoted original message, which could potentially contain the decrypted plaintext of encrypted data in the crafted email. The contents could then be transmitted to the network, either to the URL specified in the META refresh tag, or to a different URL, as the JavaScript code could modify the URL specified in the document. This bug doesn't affect users who have changed the default Message Body display setting to 'simple html' or 'plain text'. This vulnerability affects Thunderbird < 102.2.1 and Thunderbird < 91.13.1.	8.1	More Details
CVE-2022-4687	Incorrect Use of Privileged APIs in GitHub repository usememos/memos prior to 0.9.0.	8.1	More Details
CVE-2022-47943	An issue was discovered in ksmbd in the Linux kernel 5.15 through 5.19 before 5.19.2. There is an out-of-bounds read and OOPS for SMB2_WRITE, when there is a large length in the zero DataOffset case.	8.1	More Details
CVE-2022-42927	A same-origin policy violation could have allowed the theft of cross-origin URL entries, leaking the result of a redirect, via `performance.getEntries()`. This vulnerability affects Firefox < 106, Firefox ESR < 102.4, and Thunderbird < 102.4.	8.1	More Details
CVE-2022-43601	Multiple code execution vulnerabilities exist in the IFFOutput::close() functionality of OpenImageIO Project OpenImageIO v2.4.4.2. A specially crafted ImageOutput Object can lead to a heap buffer overflow. An attacker can provide malicious input to trigger these vulnerabilities.This vulnerability arises when the `ymax` variable is set to 0xFFFF and `m_spec.format` is `TypeDesc::UINT16`	8.1	More Details
CVE-2022-34469	When a TLS Certificate error occurs on a domain protected by the HSTS header, the browser should not allow the user to bypass the certificate error. On Firefox for Android, the user was presented with the option to bypass the error; this could only have been done by the user explicitly. *This bug only affects Firefox for Android. Other operating systems are unaffected.*. This vulnerability affects Firefox < 102.	8.1	More Details
CVE-2022-43600	Multiple code execution vulnerabilities exist in the IFFOutput::close() functionality of OpenImageIO Project OpenImageIO v2.4.4.2. A specially crafted ImageOutput Object can lead to a heap buffer overflow. An attacker can provide malicious input to trigger these vulnerabilities.This vulnerability arises when the `xmax` variable is set to 0xFFFF and `m_spec.format` is `TypeDesc::UINT16`	8.1	More Details
CVE-2022-43598	Multiple memory corruption vulnerabilities exist in the IFFOutput alignment padding functionality of OpenImageIO Project OpenImageIO v2.4.4.2. A specially crafted ImageOutput Object can lead to arbitrary code execution. An attacker can provide malicious input to trigger these vulnerabilities.This vulnerability arises when the `m_spec.format` is `TypeDesc::UINT16`.	8.1	More Details
CVE-2022-43597	Multiple memory corruption vulnerabilities exist in the IFFOutput alignment padding functionality of OpenImageIO Project OpenImageIO v2.4.4.2. A specially crafted ImageOutput Object can lead to arbitrary code execution. An attacker can provide malicious input to trigger these vulnerabilities.This vulnerability arises when the `m_spec.format` is `TypeDesc::UINT8`.	8.1	More Details
CVE-2022-41981	A stack-based buffer overflow vulnerability exists in the TGA file format parser of OpenImageIO v2.3.19.0. A specially-crafted targa file can lead to out of bounds read and write on the process stack, which can lead to arbitrary code execution. An attacker can provide a malicious file to trigger this vulnerability.	8.1	More Details
CVE-2022-4734	Improper Removal of Sensitive Information Before Storage or Transfer in GitHub repository usememos/memos prior to 0.9.1.	8.1	More Details

CVE Number	Description	Base Score	Reference
CVE-2019-9579	An issue was discovered in Illumos in Nexenta NexentaStor 4.0.5 and 5.1.2, and other products. The SMB server allows an attacker to have unintended access, e.g., an attacker with WRITE_XATTR can change permissions. This occurs because of a combination of three factors: ZFS extended attributes are used to implement NT named streams, the SMB protocol requires implementations to have open handle semantics similar to those of NTFS, and the SMB server passes along certain attribute requests to the underlying object (i.e., they are not considered to be requests that pertain to the named stream).	8.1	More Details
CVE-2020-10650	A deserialization flaw was discovered in jackson-databind through 2.9.10.4. It could allow an unauthenticated user to perform code execution via ignite-jta or quartz-core: org.apache.ignite.cache.jta.jndi.CacheJndiTmLookup, org.apache.ignite.cache.jta.jndi.CacheJndiTmFactory, and org.quartz.utils.JNDIConnectionProvider.	8.1	More Details
CVE-2022-43599	Multiple code execution vulnerabilities exist in the IFFOutput::close() functionality of OpenImageIO Project OpenImageIO v2.4.4.2. A specially crafted ImageOutput Object can lead to a heap buffer overflow. An attacker can provide malicious input to trigger these vulnerabilities.This vulnerability arises when the `xmax` variable is set to 0xFFFF and `m_spec.format` is `TypeDesc::UINT8`	8.1	More Details
CVE-2022-45414	If a Thunderbird user quoted from an HTML email, for example by replying to the email, and the email contained either a VIDEO tag with the POSTER attribute or an OBJECT tag with a DATA attribute, a network request to the referenced remote URL was performed, regardless of a configuration to block remote content. An image loaded from the POSTER attribute was shown in the composer window. These issues could have given an attacker additional capabilities when targetting releases that did not yet have a fix for CVE-2022-3033 which was reported around three months ago. This vulnerability affects Thunderbird < 102.5.1.	8.1	More Details
CVE-2022-46282	Use after free vulnerability in CX-Drive V3.00 and earlier allows a local attacker to execute arbitrary code by having a user to open a specially crafted file,	7.8	More Details
CVE-2022-46330	Squirrel.Windows is both a toolset and a library that provides installation and update functionality for Windows desktop applications. Installers generated by Squirrel.Windows 2.0.1 and earlier contain an issue with the DLL search path, which may lead to insecurely loading Dynamic Link Libraries. As a result, arbitrary code may be executed with the privilege of the user invoking the installer.	7.8	More Details
CVE-2022-38060	A privilege escalation vulnerability exists in the sudo functionality of OpenStack Kolla git master 05194e7618. A misconfiguration in /etc/sudoers within a container can lead to increased privileges.	7.8	More Details
CVE-2022-30260	Emerson DeltaV Distributed Control System (DCS) has insufficient verification of firmware integrity (an inadequate checksum approach, and no signature). This affects versions before 14.3 of DeltaV M-series, DeltaV S-series, DeltaV P-series, DeltaV SIS, and DeltaV CIOC/EIOC/WIOC IO cards.	7.8	More Details
CVE-2020-12069	In CODESYS V3 products in all versions prior V3.5.16.0 containing the CmpUserMgr, the CODESYS Control runtime system stores the online communication passwords using a weak hashing algorithm. This can be used by a local attacker with low privileges to gain full control of the device.	7.8	More Details
CVE-2022-0517	Mozilla VPN can load an OpenSSL configuration file from an unsecured directory. A user or attacker with limited privileges could leverage this to launch arbitrary code with SYSTEM privilege. This vulnerability affects Mozilla VPN < 2.7.1.	7.8	More Details
CVE-2022-45798	A link following vulnerability in the Damage Cleanup Engine component of Trend Micro Apex One and Trend Micro Apex One as a Service could allow a local attacker to escalate privileges by creating a symbolic link and abusing the service to delete a file. Please note: an attacker must first obtain the ability to execute low-privileged code on the target system in order to exploit this vulnerability.	7.8	More Details
CVE-2022-46334	Proofpoint Enterprise Protection (PPS/PoD) contains a vulnerability which allows the pps user to escalate to root privileges due to unnecessary permissions. This affects all versions 8.19.0 and below.	7.8	More Details
CVE-2022-45415	When downloading an HTML file, if the title of the page was formatted as a filename with a malicious extension, Firefox may have saved the file with that extension, leading to possible system compromise if the downloaded file was later ran. This vulnerability affects Firefox < 107.	7.8	More Details
CVE-2019-19705	Realtek Audio Drivers for Windows, as used on the Lenovo ThinkPad X1 Carbon 20A7, 20A8, 20BS, and 20BT before 6.0.8882.1 and 20KH and 20KG before 6.0.8907.1 (and on many other Lenovo and non-Lenovo products), mishandles DLL preloading.	7.8	More Details

CVE Number	Description	Base Score	Reference
CVE-2022-3156	A remote code execution vulnerability exists in Rockwell Automation Studio 5000 Logix Emulate software. Users are granted elevated permissions on certain product services when the software is installed. Due to this misconfiguration, a malicious user could potentially achieve remote code execution on the targeted software.	7.8	More Details
CVE-2022-3155	When saving or opening an email attachment on macOS, Thunderbird did not set attribute com.apple.quarantine on the received file. If the received file was an application and the user attempted to open it, then the application was started immediately without asking the user to confirm. This vulnerability affects Thunderbird < 102.3.	7.8	More Details
CVE-2022-37706	enlightenment_sys in Enlightenment before 0.25.4 allows local users to gain privileges because it is setuid root, and the system library function mishandles pathnames that begin with a /dev/.. substring.	7.8	More Details
CVE-2022-38658	BigFix deployments that have installed the Notification Service on Windows are susceptible to disclosing SMTP BigFix operator's sensitive data in clear text. Operators who use Notification Service related content from BES Support are at risk of leaving their SMTP sensitive data exposed.	7.7	More Details
CVE-2020-15679	An OAuth session fixation vulnerability existed in the VPN login flow, where an attacker could craft a custom login URL, convince a VPN user to login via that URL, and obtain authenticated access as that user. This issue is limited to cases where attacker and victim are sharing the same source IP and could allow the ability to view session states and disconnect VPN sessions. This vulnerability affects Mozilla VPN iOS 1.0.7 < (929), Mozilla VPN Windows < 1.2.2, and Mozilla VPN Android 1.1.0 < (1360).	7.6	More Details
CVE-2022-36319	When combining CSS properties for overflow and transform, the mouse cursor could interact with different coordinates than displayed. This vulnerability affects Firefox ESR < 102.1, Firefox ESR < 91.12, Firefox < 103, Thunderbird < 102.1, and Thunderbird < 91.12.	7.5	More Details
CVE-2022-40898	An issue discovered in Python Packaging Authority (PyPA) Wheel 0.37.1 and earlier allows remote attackers to cause a denial of service via attacker controlled input to wheel cli.	7.5	More Details
CVE-2021-35953	fastrack Reflex 2.0 W307S_REFLEX_v90.89 Activity Tracker allows a Remote attacker to cause a Denial of Service (device outage) via crafted choices of the last three bytes of a characteristic value.	7.5	More Details
CVE-2020-26302	is.js is a general-purpose check library. Versions 0.9.0 and prior contain one or more regular expressions that are vulnerable to Regular Expression Denial of Service (ReDoS). is.js uses a regex copy-pasted from a gist to validate URLs. Trying to validate a malicious string can cause the regex to loop “forever." This vulnerability was found using a CodeQL query which identifies inefficient regular expressions. is.js has no patch for this issue.	7.5	More Details
CVE-2022-28229	The hash functionality in userver before 42059b6319661583b3080cab9b595d4f8ac48128 allows attackers to cause a denial of service via crafted HTTP request, involving collisions.	7.5	More Details
CVE-2022-23854	AVEVA InTouch Access Anywhere versions 2020 R2 and older are vulnerable to a path traversal exploit that could allow an unauthenticated user with network access to read files on the system outside of the secure gateway web server.	7.5	More Details
CVE-2021-38561	golang.org/x/text/language in golang.org/x/text before 0.3.7 can panic with an out-of-bounds read during BCP 47 language tag parsing. Index calculation is mishandled. If parsing untrusted user input, this can be used as a vector for a denial-of-service attack.	7.5	More Details
CVE-2022-22184	An Improper Input Validation vulnerability in the Routing Protocol Daemon (rpd) of Juniper Networks Junos OS and Junos OS Evolved allows an unauthenticated network-based attacker to cause a Denial of Service (DoS). If a BGP update message is received over an established BGP session, and that message contains a specific, optional transitive attribute, this session will be torn down with an update message error. This issue cannot propagate beyond an affected system as the processing error occurs as soon as the update is received. This issue is exploitable remotely as the respective attribute will propagate through unaffected systems and intermediate AS (if any). Continuous receipt of a BGP update containing this attribute will create a sustained Denial of Service (DoS) condition. Since this issue only affects 22.3R1, Juniper strongly encourages customers to move to 22.3R1-S1. Juniper SIRT felt that the need to promptly warn customers about this issue affecting the 22.3R1 versions of Junos OS and Junos OS Evolved warranted an Out of Cycle JSA. This issue affects: Juniper Networks Junos OS version 22.3R1. Juniper Networks Junos OS Evolved version 22.3R1-EVO. This issue does not affect: Juniper Networks Junos OS versions prior to 22.3R1. Juniper Networks Junos OS Evolved versions prior to 22.3R1-EVO.	7.5	More Details

CVE Number	Description	Base Score	Reference
CVE-2022-45407	If an attacker loaded a font using <code>FontFace()</code> on a background worker, a use-after-free could have occurred, leading to a potentially exploitable crash. This vulnerability affects Firefox < 107.	7.5	More Details
CVE-2022-42953	Certain ZKTeco products (ZEM500-510-560-760, ZEM600-800, ZEM720, ZMM) allow access to sensitive information via direct requests for the form/DataApp?style=1 and form/DataApp?style=0 URLs. The affected versions may be before 8.88 (ZEM500-510-560-760, ZEM600-800, ZEM720) and 15.00 (ZMM200-220-210). The fixed versions are firmware version 8.88 (ZEM500-510-560-760, ZEM600-800, ZEM720) and firmware version 15.00 (ZMM200-220-210).	7.5	More Details
CVE-2022-47941	An issue was discovered in ksmbd in the Linux kernel 5.15 through 5.19 before 5.19.2. fs/ksmbd/smb2pdu.c omits a kfree call in certain smb2_handle_negotiate error conditions, aka a memory leak.	7.5	More Details
CVE-2022-33324	Improper Resource Shutdown or Release vulnerability in Mitsubishi Electric Corporation MELSEC iQ-R Series R00/01/02CPU Firmware versions "32" and prior, Mitsubishi Electric Corporation MELSEC iQ-R Series R04/08/16/32/120(EN)CPU Firmware versions "65" and prior, Mitsubishi Electric Corporation MELSEC iQ-R Series R08/16/32/120SFCPU Firmware versions "29" and prior, Mitsubishi Electric Corporation MELSEC iQ-R Series R08/16/32/120PSFCPU Firmware versions "08" and prior, Mitsubishi Electric Corporation MELSEC iQ-R Series R12CCPU-V Firmware versions "17" and prior, Mitsubishi Electric Corporation MELSEC iQ-L Series L04/08/16/32HCPU Firmware versions "05" and prior and Mitsubishi Electric Corporation MELIPC Series MI5122-VW Firmware versions "07" and prior allows a remote unauthenticated attacker to cause a Denial of Service condition in Ethernet communication on the module by sending specially crafted packets. A system reset of the module is required for recovery.	7.5	More Details
CVE-2021-44758	Heimdal before 7.7.1 allows attackers to cause a NULL pointer dereference in a SPNEGO acceptor via a preferred_mech_type of GSS_C_NO_OID and a nonzero initial_response value to send_accept.	7.5	More Details
CVE-2022-40899	An issue discovered in Python Charmers Future 0.18.2 and earlier allows remote attackers to cause a denial of service via crafted Set-Cookie header from malicious web server.	7.5	More Details
CVE-2022-44016	An issue was discovered in Simmeth Lieferantenmanager before 5.6. An attacker can download arbitrary files from the web server by abusing an API call: /DS/LM_API/api/ConfigurationService/GetImages with an "'ImagesPath":"C:\\"' value.	7.5	More Details
CVE-2022-43551	A vulnerability exists in curl <7.87.0 HSTS check that could be bypassed to trick it to keep using HTTP. Using its HSTS support, curl can be instructed to use HTTPS instead of using an insecure clear-text HTTP step even when HTTP is provided in the URL. However, the HSTS mechanism could be bypassed if the host name in the given URL first uses IDN characters that get replaced to ASCII counterparts as part of the IDN conversion. Like using the character UTF-8 U+3002 (IDEOGRAPHIC FULL STOP) instead of the common ASCII full stop (U+002E) `.`. Then in a subsequent request, it does not detect the HSTS state and makes a clear text transfer. Because it would store the info IDN encoded but look for it IDN decoded.	7.5	More Details
CVE-2022-44017	An issue was discovered in Simmeth Lieferantenmanager before 5.6. Due to errors in session management, an attacker can log back into a victim's account after the victim logged out - /LMS/LM/#main can be used for this. This is due to the credentials not being cleaned from the local storage after logout.	7.5	More Details
CVE-2022-45197	Slixmpp before 1.8.3 lacks SSL Certificate hostname validation in XMLStream, allowing an attacker to pose as any server in the eyes of Slixmpp.	7.5	More Details
CVE-2021-35065	The glob-parent package before 6.0.1 for Node.js allows ReDoS (regular expression denial of service) attacks against the enclosure regular expression.	7.5	More Details
CVE-2022-34477	The MediaError message property should be consistent to avoid leaking information about cross-origin resources; however for a same-site cross-origin resource, the message could have leaked information enabling XS-Leaks attacks. This vulnerability affects Firefox < 102.	7.5	More Details
CVE-2022-38476	A data race could occur in the <code>PK11_ChangePW</code> function, potentially leading to a use-after-free vulnerability. In Firefox, this lock protected the data when a user changed their master password. This vulnerability affects Firefox ESR < 102.2 and Thunderbird < 102.2.	7.5	More Details

CVE Number	Description	Base Score	Reference
CVE-2022-41999	A denial of service vulnerability exists in the DDS native tile reading functionality of OpenImageIO Project OpenImageIO v2.3.19.0 and v2.4.4.2. A specially-crafted .dds can lead to denial of service. An attacker can provide a malicious file to trigger this vulnerability.	7.5	More Details
CVE-2021-35951	fastrack Reflex 2.0 W307S_REFLEX_v90.89 Activity Tracker allows an Unauthenticated Remote attacker to send a malicious firmware update via BLE and brick the device.	7.5	More Details
CVE-2022-41988	An information disclosure vulnerability exists in the OpenImageIO::decode_iptc_iim() functionality of OpenImageIO Project OpenImageIO v2.3.19.0. A specially-crafted TIFF file can lead to a disclosure of sensitive information. An attacker can provide a malicious file to trigger this vulnerability.	7.5	More Details
CVE-2022-42949	Silverstripe silverstripe/subsites through 2.6.0 has Insecure Permissions.	7.5	More Details
CVE-2022-4158	The Contest Gallery WordPress plugin before 19.1.5.1, Contest Gallery Pro WordPress plugin before 19.1.5.1 do not escape the cg_Fields POST parameter before concatenating it to an SQL query in users-registry-check-registering-and-login.php. This may allow malicious visitors to leak sensitive information from the site's database.	7.5	More Details
CVE-2013-10005	The RemoteAddr and LocalAddr methods on the returned net.Conn may call themselves, leading to an infinite loop which will crash the program due to a stack overflow.	7.5	More Details
CVE-2020-36564	Due to improper validation of caller input, validation is silently disabled if the provided expected token is malformed, causing any user supplied token to be considered valid.	7.5	More Details
CVE-2022-22737	Constructing audio sinks could have lead to a race condition when playing audio files and closing windows. This could have lead to a use-after-free causing a potentially exploitable crash. This vulnerability affects Firefox ESR < 91.5, Firefox < 96, and Thunderbird < 91.5.	7.5	More Details
CVE-2020-36559	Due to improper sanitization of user input, HTTPEngine.Handle allows for directory traversal, allowing an attacker to read files outside of the target directory that the server has permission to read.	7.5	More Details
CVE-2019-25073	Improper path sanitization in github.com/goadesign/goa before v3.0.9, v2.0.10, or v1.4.3 allow remote attackers to read files outside of the intended directory.	7.5	More Details
CVE-2019-25072	Due to support of Gzip compression in request bodies, as well as a lack of limiting response body sizes, a malicious server can cause a client to consume a significant amount of system resources, which may be used as a denial of service vector.	7.5	More Details
CVE-2015-10004	Token validation methods are susceptible to a timing side-channel during HMAC comparison. With a large enough number of requests over a low latency connection, an attacker may use this to determine the expected HMAC.	7.5	More Details
CVE-2022-4156	The Contest Gallery WordPress plugin before 19.1.5.1, Contest Gallery Pro WordPress plugin before 19.1.5.1 do not escape the user_id POST parameter before concatenating it to an SQL query in ajax-functions-backend.php. This may allow malicious users with at least author privilege to leak sensitive information from the site's database.	7.5	More Details
CVE-2020-12067	In Pilz PMC programming tool 3.x before 3.5.17 (based on CODESYS Development System), a user's password may be changed by an attacker without knowledge of the current password.	7.5	More Details
CVE-2022-4767	Denial of Service in GitHub repository usememos/memos prior to 0.9.1.	7.5	More Details
CVE-2020-36567	Unsanitized input in the default logger in github.com/gin-gonic/gin before v1.6.0 allows remote attackers to inject arbitrary log lines.	7.5	More Details

CVE Number	Description	Base Score	Reference
CVE-2022-45423	Some Dahua software products have a vulnerability of unauthenticated request of MQTT credentials. An attacker can obtain encrypted MQTT credentials by sending a specific crafted packet to the vulnerable interface (the credentials cannot be directly exploited).	7.5	More Details
CVE-2022-45431	Some Dahua software products have a vulnerability of unauthenticated restart of remote DSS Server. After bypassing the firewall access control policy, by sending a specific crafted packet to the vulnerable interface, an attacker could unauthenticated restart of remote DSS Server.	7.5	More Details
CVE-2022-22741	When resizing a popup while requesting fullscreen access, the popup would have become unable to leave fullscreen mode. This vulnerability affects Firefox ESR < 91.5, Firefox < 96, and Thunderbird < 91.5.	7.5	More Details
CVE-2022-45429	Some Dahua software products have a vulnerability of server-side request forgery (SSRF). An Attacker can access internal resources by concatenating links (URL) that conform to specific rules.	7.5	More Details
CVE-2020-36568	Unsanitized input in the query parser in github.com/revel/revel before v1.0.0 allows remote attackers to cause resource exhaustion via memory allocation.	7.5	More Details
CVE-2022-47581	Isode M-Vault 16.0v0 through 17.x before 17.0v24 can crash upon an LDAP v1 bind request.	7.5	More Details
CVE-2022-45425	Some Dahua software products have a vulnerability of using of hard-coded cryptographic key. An attacker can obtain the AES crypto key by exploiting this vulnerability.	7.5	More Details
CVE-2022-26387	When installing an add-on, Firefox verified the signature before prompting the user; but while the user was confirming the prompt, the underlying add-on file could have been modified and Firefox would not have noticed. This vulnerability affects Firefox < 98, Firefox ESR < 91.7, and Thunderbird < 91.7.	7.5	More Details
CVE-2022-25895	All versions of package lite-dev-server are vulnerable to Directory Traversal due to missing input sanitization and sandboxes being employed to the req.url user input that is passed to the server code.	7.5	More Details
CVE-2022-3064	Parsing malicious or large YAML documents can consume excessive amounts of CPU or memory.	7.5	More Details
CVE-2022-2584	The dag-pb codec can panic when decoding invalid blocks.	7.5	More Details
CVE-2021-4239	The Noise protocol implementation suffers from weakened cryptographic security after encrypting 2^64 messages, and a potential denial of service attack. After 2^64 (~18.4 quintillion) messages are encrypted with the Encrypt function, the nonce counter will wrap around, causing multiple messages to be encrypted with the same key and nonce. In a separate issue, the Decrypt function increments the nonce state even when it fails to decrypt a message. If an attacker can provide an invalid input to the Decrypt function, this will cause the nonce state to desynchronize between the peers, resulting in a failure to encrypt all subsequent messages.	7.5	More Details
CVE-2022-26964	Weak password derivation for export in Devolutions Remote Desktop Manager before 2022.1 allows information disclosure via a password brute-force attack. An error caused base64 to be decoded.	7.4	More Details
CVE-2022-24431	All versions of package abacus-ext-cmdline are vulnerable to Command Injection via the execute function due to improper user-input sanitization.	7.4	More Details
CVE-2022-4739	A vulnerability classified as critical was found in SourceCodester School Dormitory Management System 1.0. Affected by this vulnerability is an unknown functionality of the component Admin Login. The manipulation leads to sql injection. The attack can be launched remotely. The associated identifier of this vulnerability is VDB-216775.	7.3	More Details

CVE Number	Description	Base Score	Reference
CVE-2022-4737	A vulnerability was found in SourceCodester Blood Bank Management System 1.0. It has been rated as critical. This issue affects some unknown processing of the file login.php. The manipulation of the argument username/password leads to sql injection. The attack may be initiated remotely. The identifier VDB-216773 was assigned to this vulnerability.	7.3	More Details
CVE-2022-46570	D-Link DIR-882 DIR882A1_FW130B06, DIR-878 DIR_878_FW1.30B08 was discovered to contain a stack overflow via the Password parameter in the SetWan3Settings module.	7.2	More Details
CVE-2022-4268	The Plugin Logic WordPress plugin before 1.0.8 does not sanitise and escape a parameter before using it in a SQL statement, leading to a SQL injection exploitable by high privilege users such as admin	7.2	More Details
CVE-2022-45889	Planet eStream before 6.72.10.07 allows a remote attacker (who is a publisher or admin) to obtain access to all records stored in the database, and achieve the ability to execute arbitrary SQL commands, via Search (the StatisticsResults.aspx flt parameter).	7.2	More Details
CVE-2022-46561	D-Link DIR-882 DIR882A1_FW130B06, DIR-878 DIR_878_FW1.30B08 was discovered to contain a stack overflow via the Password parameter in the SetWanSettings module.	7.2	More Details
CVE-2022-46560	D-Link DIR-882 DIR882A1_FW130B06, DIR-878 DIR_878_FW1.30B08 was discovered to contain a stack overflow via the Password parameter in the SetWan2Settings module.	7.2	More Details
CVE-2021-24942	The Menu Item Visibility Control WordPress plugin through 0.5 doesn't sanitize and validate the "Visibility logic" option for WordPress menu items, which could allow highly privileged users to execute arbitrary PHP code even in a hardened environment.	7.2	More Details
CVE-2022-4732	Unrestricted Upload of File with Dangerous Type in GitHub repository microweber/microweber prior to 1.3.2.	7.2	More Details
CVE-2022-46568	D-Link DIR-882 DIR882A1_FW130B06, DIR-878 DIR_878_FW1.30B08 was discovered to contain a stack overflow via the AccountPassword parameter in the SetSysEmailSettings module.	7.2	More Details
CVE-2022-46566	D-Link DIR-882 DIR882A1_FW130B06, DIR-878 DIR_878_FW1.30B08 was discovered to contain a stack overflow via the Password parameter in the SetQuickVPNSettings module.	7.2	More Details
CVE-2022-4722	Authentication Bypass by Primary Weakness in GitHub repository ikus060/rdiffweb prior to 2.5.5.	7.2	More Details
CVE-2022-46563	D-Link DIR-882 DIR882A1_FW130B06, DIR-878 DIR_878_FW1.30B08 was discovered to contain a stack overflow via the Password parameter in the SetDynamicDNSSettings module.	7.2	More Details
CVE-2022-38757	A vulnerability has been identified in Micro Focus ZENworks 2020 Update 3a and prior versions. This vulnerability allows administrators with rights to perform actions (e.g., install a bundle) on a set of managed devices, to be able to exercise these rights on managed devices in the ZENworks zone but which are outside the scope of the administrator. This vulnerability does not result in the administrators gaining additional rights on the managed devices, either in the scope or outside the scope of the administrator.	7.2	More Details
CVE-2022-45427	Some Dahua software products have a vulnerability of unrestricted upload of file. After obtaining the permissions of administrators, by sending a specific crafted packet to the vulnerable interface, an attacker can upload arbitrary files.	7.2	More Details
CVE-2022-46562	D-Link DIR-882 DIR882A1_FW130B06, DIR-878 DIR_878_FW1.30B08 was discovered to contain a stack overflow via the PSK parameter in the SetQuickVPNSettings module.	7.2	More Details

CVE Number	Description	Base Score	Reference
CVE-2022-46569	D-Link DIR-882 DIR882A1_FW130B06, DIR-878 DIR_878_FW1.30B08 was discovered to contain a stack overflow via the Key parameter in the SetWLanRadioSecurity module.	7.2	More Details
CVE-2022-42930	If two Workers were simultaneously initializing their CacheStorage, a data race could have occurred in the `ThirdPartyUtil` component. This vulnerability affects Firefox < 106.	7.1	More Details
CVE-2022-46175	JSON5 is an extension to the popular JSON file format that aims to be easier to write and maintain by hand (e.g. for config files). The `parse` method of the JSON5 library before and including versions 1.0.1 and 2.2.1 does not restrict parsing of keys named `__proto__`, allowing specially crafted strings to pollute the prototype of the resulting object. This vulnerability pollutes the prototype of the object returned by `JSON5.parse` and not the global Object prototype, which is the commonly understood definition of Prototype Pollution. However, polluting the prototype of a single object can have significant security impact for an application if the object is later used in trusted operations. This vulnerability could allow an attacker to set arbitrary and unexpected keys on the object returned from `JSON5.parse`. The actual impact will depend on how applications utilize the returned object and how they filter unwanted keys, but could include denial of service, cross-site scripting, elevation of privilege, and in extreme cases, remote code execution. `JSON5.parse` should restrict parsing of `__proto__` keys when parsing JSON strings to objects. As a point of reference, the `JSON.parse` method included in JavaScript ignores `__proto__` keys. Simply changing `JSON5.parse` to `JSON.parse` in the examples above mitigates this vulnerability. This vulnerability is patched in json5 versions 1.0.2, 2.2.2, and later.	7.1	More Details
CVE-2022-22753	A Time-of-Check Time-of-Use bug existed in the Maintenance (Updater) Service that could be abused to grant Users write access to an arbitrary directory. This could have been used to escalate to SYSTEM access. *This bug only affects Firefox on Windows. Other operating systems are unaffected.*. This vulnerability affects Firefox < 97, Thunderbird < 91.6, and Firefox ESR < 91.6.	7.1	More Details
CVE-2022-23556	CodeIgniter is a PHP full-stack web framework. This vulnerability may allow attackers to spoof their IP address when the server is behind a reverse proxy. This issue has been patched, please upgrade to version 4.2.11 or later, and configure `Config\App::$proxyIPs`. As a workaround, do not use `$request->getIPAddress()`.	7.0	More Details
CVE-2022-22736	If Firefox was installed to a world-writable directory, a local privilege escalation could occur when Firefox searched the current directory for system libraries. However the install directory is not world-writable by default. *This bug only affects Firefox for Windows in a non-default installation. Other operating systems are unaffected.*. This vulnerability affects Firefox < 96.	7.0	More Details
CVE-2022-46171	Tauri is a framework for building binaries for all major desktop platforms. The filesystem glob pattern wildcards `*`, `?`, and `[...]` match file path literals and leading dots by default, which unintentionally exposes sub folder content of allowed paths. Scopes without the wildcards are not affected. As `**` allows for sub directories the behavior there is also as expected. The issue has been patched in the latest release and was backported into the currently supported 1.x branches. There are no known workarounds at the time of publication.	6.8	More Details
CVE-2022-46662	Roxio Creator LJB starts another program with an unquoted file path. Since a registered Windows service path contains spaces and are unquoted, if a malicious executable is placed on a certain path, the executable may be executed with the privilege of the Windows service. The affected product and versions are as follows: Roxio Creator LJB version number 12.2 build number 106B62B, version number 12.2 build number 106B63A, version number 12.2 build number 106B69A, version number 12.2 build number 106B71A, and version number 12.2 build number 106B74A)	6.7	More Details
CVE-2021-36631	Untrusted search path vulnerability in Baidunetdisk Version 7.4.3 and earlier allows an attacker to gain privileges via a Trojan horse DLL in an unspecified directory.	6.7	More Details
CVE-2022-45419	If the user added a security exception for an invalid TLS certificate, opened an ongoing TLS connection with a server that used that certificate, and then deleted the exception, Firefox would have kept the connection alive, making it seem like the certificate was still trusted. This vulnerability affects Firefox < 107.	6.5	More Details
CVE-2022-45420	Use tables inside of an iframe, an attacker could have caused iframe contents to be rendered outside the boundaries of the iframe, resulting in potential user confusion or spoofing attacks. This vulnerability affects Firefox ESR < 102.5, Thunderbird < 102.5, and Firefox < 107.	6.5	More Details
CVE-2022-4239	The Workreap WordPress theme before 2.6.4 does not verify that an addon service belongs to the user issuing the request, or indeed that it is an addon service, when processing the workreap_addons_service_remove action, allowing any user to delete any post by knowing or guessing the id.	6.5	More Details

CVE Number	Description	Base Score	Reference
CVE-2022-46880	A missing check related to tex units could have led to a use-after-free and potentially exploitable crash. *Note*: This advisory was added on December 13th, 2022 after we better understood the impact of the issue. The fix was included in the original release of Firefox 105. This vulnerability affects Firefox ESR < 102.6, Firefox < 105, and Thunderbird < 102.6.	6.5	More Details
CVE-2022-45416	Keyboard events reference strings like "KeyA" that were at fixed, known, and widely-spread addresses. Cache-based timing attacks such as Prime+Probe could have possibly figured out which keys were being pressed. This vulnerability affects Firefox ESR < 102.5, Thunderbird < 102.5, and Firefox < 107.	6.5	More Details
CVE-2022-47933	Brave Browser before 1.42.51 allowed a remote attacker to cause a denial of service via a crafted HTML file that references the IPFS scheme. This vulnerability is caused by an uncaught exception in the function ipfs::OnBeforeURLRequest_IPFSRedirectWork() in ipfs_redirect_network_delegate_helper.cc.	6.5	More Details
CVE-2022-4266	The Bulk Delete Users by Email WordPress plugin through 1.2 does not have CSRF check when deleting users, which could allow attackers to make a logged in admin delete non admin users by knowing their email via a CSRF attack	6.5	More Details
CVE-2022-47934	Brave Browser before 1.43.88 allowed a remote attacker to cause a denial of service in private and guest windows via a crafted HTML file that mentions an ipfs:// or ipns:// URL. This is caused by an incomplete fix for CVE-2022-47932 and CVE-2022-47934.	6.5	More Details
CVE-2022-28282	By using a link with <code>rel="localization"</code> a use-after-free could have been triggered by destroying an object during JavaScript execution and then referencing the object through a freed pointer, leading to a potential exploitable crash. This vulnerability affects Thunderbird < 91.8, Firefox < 99, and Firefox ESR < 91.8.	6.5	More Details
CVE-2022-4166	The Contest Gallery WordPress plugin before 19.1.5.1, Contest Gallery Pro WordPress plugin before 19.1.5.1 do not escape the addCountS POST parameter before concatenating it to an SQL query in 4_activate.php. This may allow malicious users with at least author privilege to leak sensitive information from the site's database.	6.5	More Details
CVE-2022-46875	The executable file warning was not presented when downloading .atloc and .ftploc files, which can run commands on a user's computer. *Note: This issue only affected Mac OS operating systems. Other operating systems are unaffected.*. This vulnerability affects Firefox < 108, Firefox ESR < 102.6, and Thunderbird < 102.6.	6.5	More Details
CVE-2022-4646	Cross-Site Request Forgery (CSRF) in GitHub repository ikus060/rdiffweb prior to 2.5.4.	6.5	More Details
CVE-2022-46491	A Cross-Site Request Forgery (CSRF) vulnerability in the Add Administrator function of the default version of nbnbk allows attackers to arbitrarily add Administrator accounts.	6.5	More Details
CVE-2019-18177	In certain Citrix products, information disclosure can be achieved by an authenticated VPN user when there is a configured SSL VPN endpoint. This affects Citrix ADC and Citrix Gateway 13.0-58.30 and later releases before the CTX276688 update.	6.5	More Details
CVE-2019-13988	Sierra Wireless MGOS before 3.15.2 and 4.x before 4.3 allows attackers to read log files via a Direct Request (aka Forced Browsing).	6.5	More Details
CVE-2022-45426	Some Dahua software products have a vulnerability of unrestricted download of file. After obtaining the permissions of ordinary users, by sending a specific crafted packet to the vulnerable interface, an attacker can download arbitrary files.	6.5	More Details
CVE-2018-16135	The Opera Mini application 47.1.2249.129326 for Android allows remote attackers to spoof the Location Permission dialog via a crafted web site.	6.5	More Details
CVE-2022-44014	An issue was discovered in Simmeth Lieferantenmanager before 5.6. In the design of the API, a user is inherently able to fetch arbitrary SQL tables. This leaks all user passwords and MSSQL hashes via /DS/LM_API/api/SelectionService/GetPaggedTab.	6.5	More Details
CVE-2022-47938	An issue was discovered in ksmbd in the Linux kernel 5.15 through 5.19 before 5.19.2. fs/ksmbd/smb2misc.c has an out-of-bounds read and OOPS for SMB2_TREE_CONNECT.	6.5	More Details

CVE Number	Description	Base Score	Reference
CVE-2022-23547	PJSIP is a free and open source multimedia communication library written in C language implementing standard based protocols such as SIP, SDP, RTP, STUN, TURN, and ICE. This issue is similar to GHSA-9pfh-r8x4-w26w. Possible buffer overread when parsing a certain STUN message. The vulnerability affects applications that uses STUN including PJNATH and PJSUA-LIB. The patch is available as commit in the master branch.	6.5	More Details
CVE-2022-4723	Allocation of Resources Without Limits or Throttling in GitHub repository ikus060/rdiffweb prior to 2.5.5.	6.5	More Details
CVE-2022-41317	An issue was discovered in Squid 4.9 through 4.17 and 5.0.6 through 5.6. Due to inconsistent handling of internal URIs, there can be Exposure of Sensitive Information about clients using the proxy via an HTTPS request to an internal cache manager URL. This is fixed in 5.7.	6.5	More Details
CVE-2022-4683	Sensitive Cookie in HTTPS Session Without 'Secure' Attribute in GitHub repository usememos/memos prior to 0.9.0.	6.5	More Details
CVE-2022-46492	nbnbk commit 879858451d53261d10f77d4709aee2d01c72c301 was discovered to contain an arbitrary file read vulnerability via the component /api/Index/getFileBinary.	6.5	More Details
CVE-2022-36221	Nokia Fastmile 3tg00118abad52 is affected by an authenticated path traversal vulnerability which allows attackers to read any named pipe file on the system.	6.5	More Details
CVE-2022-45410	When a ServiceWorker intercepted a request with <code>FetchEvent</code>, the origin of the request was lost after the ServiceWorker took ownership of it. This had the effect of negating SameSite cookie protections. This was addressed in the spec and then in browsers. This vulnerability affects Firefox ESR < 102.5, Thunderbird < 102.5, and Firefox < 107.	6.5	More Details
CVE-2022-45894	GetFile.aspx in Planet eStream before 6.72.10.07 allows ..\ directory traversal to read arbitrary local files.	6.5	More Details
CVE-2022-45895	Planet eStream before 6.72.10.07 discloses sensitive information, related to the ON cookie (findable in HTML source code for Default.aspx in some situations) and the WhoAmI endpoint (e.g., path disclosure).	6.5	More Details
CVE-2022-4165	The Contest Gallery WordPress plugin before 19.1.5.1, Contest Gallery Pro WordPress plugin before 19.1.5.1 do not escape the cg_order POST parameter before concatenating it to an SQL query in order-custom-fields-with-and-without-search.php. This may allow malicious users with at least author privilege to leak sensitive information from the site's database.	6.5	More Details
CVE-2022-28283	The sourceMapURL feature in devtools was missing security checks that would have allowed a webpage to attempt to include local files or other files that should have been inaccessible. This vulnerability affects Firefox < 99.	6.5	More Details
CVE-2022-4164	The Contest Gallery WordPress plugin before 19.1.5.1, Contest Gallery Pro WordPress plugin before 19.1.5.1 do not escape the cg_multiple_files_for_post POST parameter before concatenating it to an SQL query in 0_change-gallery.php. This may allow malicious users with at least author privilege to leak sensitive information from the site's database.	6.5	More Details
CVE-2021-39369	In Philips (formerly Carestream) Vue MyVue PACS through 12.2.x.x, the VideoStream function allows Path Traversal by authenticated users to access files stored outside of the web root.	6.5	More Details
CVE-2022-34478	The <code>ms-msdt</code>, <code>search</code>, and <code>search-ms</code> protocols deliver content to Microsoft applications, bypassing the browser, when a user accepts a prompt. These applications have had known vulnerabilities, exploited in the wild (although we know of none exploited through Thunderbird), so in this release Thunderbird has blocked these protocols from prompting the user to open them. *This bug only affects Thunderbird on Windows. Other operating systems are unaffected.*. This vulnerability affects Firefox < 102, Firefox ESR < 91.11, Thunderbird < 102, and Thunderbird < 91.11.	6.5	More Details

CVE Number	Description	Base Score	Reference
CVE-2022-22760	When importing resources using Web Workers, error messages would distinguish the difference between <code>application/javascript</code> responses and non-script responses. This could have been abused to learn information cross-origin. This vulnerability affects Firefox < 97, Thunderbird < 91.6, and Firefox ESR < 91.6.	6.5	More Details
CVE-2022-4162	The Contest Gallery WordPress plugin before 19.1.5.1, Contest Gallery Pro WordPress plugin before 19.1.5.1 do not escape the cg_row POST parameter before concatenating it to an SQL query in 3_row-order.php. This may allow malicious users with at least author privilege to leak sensitive information from the site's database.	6.5	More Details
CVE-2022-4161	The Contest Gallery WordPress plugin before 19.1.5.1, Contest Gallery Pro WordPress plugin before 19.1.5.1 do not escape the cg_copy_start POST parameter before concatenating it to an SQL query in copy-gallery-images.php. This may allow malicious users with at least author privilege to leak sensitive information from the site's database.	6.5	More Details
CVE-2022-22757	Remote Agent, used in WebDriver, did not validate the Host or Origin headers. This could have allowed websites to connect back locally to the user's browser to control it. *This bug only affected Firefox when WebDriver was enabled, which is not the default configuration.*. This vulnerability affects Firefox < 97.	6.5	More Details
CVE-2022-1834	When displaying the sender of an email, and the sender name contained the Braille Pattern Blank space character multiple times, Thunderbird would have displayed all the spaces. This could have been used by an attacker to send an email message with the attacker's digital signature, that was shown with an arbitrary sender email address chosen by the attacker. If the sender name started with a false email address, followed by many Braille space characters, the attacker's email address was not visible. Because Thunderbird compared the invisible sender address with the signature's email address, if the signing key or certificate was accepted by Thunderbird, the email was shown as having a valid digital signature. This vulnerability affects Thunderbird < 91.10.	6.5	More Details
CVE-2022-3032	When receiving an HTML email that contained an <code>iframe</code> element, which used a <code>srcdoc</code> attribute to define the inner HTML document, remote objects specified in the nested document, for example images or videos, were not blocked. Rather, the network was accessed, the objects were loaded and displayed. This vulnerability affects Thunderbird < 102.2.1 and Thunderbird < 91.13.1.	6.5	More Details
CVE-2022-22754	If a user installed an extension of a particular type, the extension could have auto-updated itself and while doing so, bypass the prompt which grants the new version the new requested permissions. This vulnerability affects Firefox < 97, Thunderbird < 91.6, and Firefox ESR < 91.6.	6.5	More Details
CVE-2022-31742	An attacker could have exploited a timing attack by sending a large number of allowCredential entries and detecting the difference between invalid key handles and cross-origin key handles. This could have led to cross-origin account linking in violation of WebAuthn goals. This vulnerability affects Thunderbird < 91.10, Firefox < 101, and Firefox ESR < 91.10.	6.5	More Details
CVE-2022-4160	The Contest Gallery WordPress plugin before 19.1.5.1, Contest Gallery Pro WordPress plugin before 19.1.5.1 do not escape the cg_copy_id POST parameter before concatenating it to an SQL query in cg-copy-comments.php and cg-copy-rating.php. This may allow malicious users with at least author privilege to leak sensitive information from the site's database.	6.5	More Details
CVE-2022-31743	Firefox's HTML parser did not correctly interpret HTML comment tags, resulting in an incongruity with other browsers. This could have been used to escape HTML comments on pages that put user-controlled data in them. This vulnerability affects Firefox < 101.	6.5	More Details
CVE-2022-38475	An attacker could have written a value to the first element in a zero-length JavaScript array. Although the array was zero-length, the value was not written to an invalid memory address. This vulnerability affects Firefox < 104.	6.5	More Details
CVE-2022-22739	Malicious websites could have tricked users into accepting launching a program to handle an external URL protocol. This vulnerability affects Firefox ESR < 91.5, Firefox < 96, and Thunderbird < 91.5.	6.5	More Details
CVE-2022-2226	An OpenPGP digital signature includes information about the date when the signature was created. When displaying an email that contains a digital signature, the email's date will be shown. If the dates were different, then Thunderbird didn't report the email as having an invalid signature. If an attacker performed a replay attack, in which an old email with old contents are resent at a later time, it could lead the victim to believe that the statements in the email are current. Fixed versions of Thunderbird will require that the signature's date roughly matches the displayed date of the email. This vulnerability affects Thunderbird < 102 and Thunderbird < 91.11.	6.5	More Details
CVE-2022-31744	An attacker could have injected CSS into stylesheets accessible via internal URIs, such as resource:, and in doing so bypass a page's Content Security Policy. This vulnerability affects Firefox ESR < 91.11, Thunderbird < 102, Thunderbird < 91.11, and Firefox < 101.	6.5	More Details

CVE Number	Description	Base Score	Reference
CVE-2022-38472	An attacker could have abused XSLT error handling to associate attacker-controlled content with another origin which was displayed in the address bar. This could have been used to fool the user into submitting data intended for the spoofed origin. This vulnerability affects Thunderbird < 102.2, Thunderbird < 91.13, Firefox ESR < 91.13, Firefox ESR < 102.2, and Firefox < 104.	6.5	More Details
CVE-2022-36317	When visiting a website with an overly long URL, the user interface would start to hang. Due to session restore, this could lead to a permanent Denial of Service. *This bug only affects Firefox for Android. Other operating systems are unaffected.*. This vulnerability affects Firefox < 103.	6.5	More Details
CVE-2022-31746	Internal URLs are protected by a secret UUID key, which could have been leaked to web page through the Referrer header. This vulnerability affects Firefox for iOS < 102.	6.5	More Details
CVE-2022-22742	When inserting text while in edit mode, some characters might have lead to out-of-bounds memory access causing a potentially exploitable crash. This vulnerability affects Firefox ESR < 91.5, Firefox < 96, and Thunderbird < 91.5.	6.5	More Details
CVE-2022-47932	Brave Browser before 1.43.34 allowed a remote attacker to cause a denial of service via a crafted HTML file that mentions an ipfs:// or ipns:// URL. This vulnerability is caused by an incomplete fix for CVE-2022-47933.	6.5	More Details
CVE-2022-34471	When downloading an update for an addon, the downloaded addon update's version was not verified to match the version selected from the manifest. If the manifest had been tampered with on the server, an attacker could trick the browser into downgrading the addon to a prior version. This vulnerability affects Firefox < 102.	6.5	More Details
CVE-2022-22750	By generally accepting and passing resource handles across processes, a compromised content process might have confused higher privileged processes to interact with handles that the unprivileged process should not have access to. *This bug only affects Firefox for Windows and MacOS. Other operating systems are unaffected.*. This vulnerability affects Firefox < 96.	6.5	More Details
CVE-2022-4159	The Contest Gallery WordPress plugin before 19.1.5.1, Contest Gallery Pro WordPress plugin before 19.1.5.1 do not escape the cg_id POST parameter before concatenating it to an SQL query in 0_change-gallery.php. This may allow malicious users with at least author privilege to leak sensitive information from the site's database.	6.5	More Details
CVE-2022-22745	Securitypolicyviolation events could have leaked cross-origin information for frame-ancestors violations. This vulnerability affects Firefox ESR < 91.5, Firefox < 96, and Thunderbird < 91.5.	6.5	More Details
CVE-2022-22747	After accepting an untrusted certificate, handling an empty pkcs7 sequence as part of the certificate data could have lead to a crash. This crash is believed to be unexploitable. This vulnerability affects Firefox ESR < 91.5, Firefox < 96, and Thunderbird < 91.5.	6.5	More Details
CVE-2022-22748	Malicious websites could have confused Firefox into showing the wrong origin when asking to launch a program and handling an external URL protocol. This vulnerability affects Firefox ESR < 91.5, Firefox < 96, and Thunderbird < 91.5.	6.5	More Details
CVE-2022-4153	The Contest Gallery WordPress plugin before 19.1.5.1, Contest Gallery Pro WordPress plugin before 19.1.5.1 do not escape the upload[] POST parameter before concatenating it to an SQL query in get-data-create-upload-v10.php. This may allow malicious users with at least author privilege to leak sensitive information from the site's database.	6.5	More Details
CVE-2022-31738	When exiting fullscreen mode, an iframe could have confused the browser about the current state of fullscreen, resulting in potential user confusion or spoofing attacks. This vulnerability affects Thunderbird < 91.10, Firefox < 101, and Firefox ESR < 91.10.	6.5	More Details
CVE-2022-4152	The Contest Gallery WordPress plugin before 19.1.5, Contest Gallery Pro WordPress plugin before 19.1.5 do not escape the option_id POST parameter before concatenating it to an SQL query in edit-options.php. This may allow malicious users with at least author privilege to leak sensitive information from the site's database.	6.5	More Details
CVE-2022-40961	During startup, a graphics driver with an unexpected name could lead to a stack-buffer overflow causing a potentially exploitable crash. *This issue only affects Firefox for Android. Other operating systems are not affected.*. This vulnerability affects Firefox < 105.	6.5	More Details
CVE-2022-45408	Through a series of popups that reuse windowName, an attacker can cause a window to go fullscreen without the user seeing the notification prompt, resulting in potential user confusion or spoofing attacks. This vulnerability affects Firefox ESR < 102.5, Thunderbird < 102.5, and Firefox < 107.	6.5	More Details

CVE Number	Description	Base Score	Reference
CVE-2022-28285	When generating the assembly code for <code>MLoadTypedArrayElementHole</code>, an incorrect AliasSet was used. In conjunction with another vulnerability this could have been used for an out of bounds memory read. This vulnerability affects Thunderbird < 91.8, Firefox < 99, and Firefox ESR < 91.8.	6.5	More Details
CVE-2022-45405	Freeing arbitrary <code>nsIInputStream</code>'s on a different thread than creation could have led to a use-after-free and potentially exploitable crash. This vulnerability affects Firefox ESR < 102.5, Thunderbird < 102.5, and Firefox < 107.	6.5	More Details
CVE-2022-45404	Through a series of popup and <code>window.print()</code> calls, an attacker can cause a window to go fullscreen without the user seeing the notification prompt, resulting in potential user confusion or spoofing attacks. This vulnerability affects Firefox ESR < 102.5, Thunderbird < 102.5, and Firefox < 107.	6.5	More Details
CVE-2022-4150	The Contest Gallery WordPress plugin before 19.1.5.1, Contest Gallery Pro WordPress plugin before 19.1.5.1 do not escape the option_id POST parameter before concatenating it to an SQL query in order-custom-fields-with-and-without-search.php. This may allow malicious users with at least author privilege to leak sensitive information from the site's database.	6.5	More Details
CVE-2022-45403	Service Workers should not be able to infer information about opaque cross-origin responses; but timing information for cross-origin media combined with Range requests might have allowed them to determine the presence or length of a media file. This vulnerability affects Firefox ESR < 102.5, Thunderbird < 102.5, and Firefox < 107.	6.5	More Details
CVE-2021-4126	When receiving an OpenPGP/MIME signed email message that contains an additional outer MIME message layer, for example a message footer added by a mailing list gateway, Thunderbird only considered the inner signed message for the signature validity. This gave the false impression that the additional contents were also covered by the digital signature. Starting with Thunderbird version 91.4.1, only the signature that belongs to the top level MIME part will be considered for the displayed status. This vulnerability affects Thunderbird < 91.4.1.	6.5	More Details
CVE-2022-42929	If a website called `window.print()` in a particular way, it could cause a denial of service of the browser, which may persist beyond browser restart depending on the user's session restore settings. This vulnerability affects Firefox < 106, Firefox ESR < 102.4, and Thunderbird < 102.4.	6.5	More Details
CVE-2022-28287	In unusual circumstances, selecting text could cause text selection caching to behave incorrectly, leading to a crash. This vulnerability affects Firefox < 99.	6.5	More Details
CVE-2021-4128	When transitioning in and out of fullscreen mode, a graphics object was not correctly protected; resulting in memory corruption and a potentially exploitable crash. *This bug only affects Firefox on MacOS. Other operating systems are unaffected.*. This vulnerability affects Firefox < 95.	6.5	More Details
CVE-2022-4163	The Contest Gallery WordPress plugin before 19.1.5.1, Contest Gallery Pro WordPress plugin before 19.1.5.1 do not escape the cg_deactivate and cg_activate POST parameters before concatenating it to an SQL query in 2_deactivate.php and 4_activate.php, respectively. This may allow malicious users with at least author privilege to leak sensitive information from the site's database.	6.5	More Details
CVE-2022-4151	The Contest Gallery WordPress plugin before 19.1.5.1, Contest Gallery Pro WordPress plugin before 19.1.5.1 do not escape the option_id GET parameter before concatenating it to an SQL query in export-images-data.php. This may allow malicious users with at least author privilege to leak sensitive information from the site's database.	6.5	More Details
CVE-2022-1097	<code>NSSToken</code> objects were referenced via direct points, and could have been accessed in an unsafe way on different threads, leading to a use-after-free and potentially exploitable crash. This vulnerability affects Thunderbird < 91.8, Firefox < 99, and Firefox ESR < 91.8.	6.5	More Details
CVE-2022-26386	Previously Firefox for macOS and Linux would download temporary files to a user-specific directory in <code>/tmp</code>, but this behavior was changed to download them to <code>/tmp</code> where they could be affected by other local users. This behavior was reverted to the original, user-specific directory. *This bug only affects Firefox for macOS and Linux. Other operating systems are unaffected.*. This vulnerability affects Firefox ESR < 91.7 and Thunderbird < 91.7.	6.5	More Details
CVE-2022-40957	Inconsistent data in instruction and data cache when creating wasm code could lead to a potentially exploitable crash. *This bug only affects Firefox on ARM64 platforms.*. This vulnerability affects Firefox ESR < 102.3, Thunderbird < 102.3, and Firefox < 105.	6.5	More Details
CVE-2022-1196	After a VR Process is destroyed, a reference to it may have been retained and used, leading to a use-after-free and potentially exploitable crash. This vulnerability affects Thunderbird < 91.8 and Firefox ESR < 91.8.	6.5	More Details

CVE Number	Description	Base Score	Reference
CVE-2022-29916	Firefox behaved slightly differently for already known resources when loading CSS resources involving CSS variables. This could have been used to probe the browser history. This vulnerability affects Thunderbird < 91.9, Firefox ESR < 91.9, and Firefox < 100.	6.5	More Details
CVE-2022-29914	When reusing existing popups Firefox would have allowed them to cover the fullscreen notification UI, which could have enabled browser spoofing attacks. This vulnerability affects Thunderbird < 91.9, Firefox ESR < 91.9, and Firefox < 100.	6.5	More Details
CVE-2022-40960	Concurrent use of the URL parser with non-UTF-8 data was not thread-safe. This could lead to a use-after-free causing a potentially exploitable crash. This vulnerability affects Firefox ESR < 102.3, Thunderbird < 102.3, and Firefox < 105.	6.5	More Details
CVE-2022-29913	The parent process would not properly check whether the Speech Synthesis feature is enabled, when receiving instructions from a child process. This vulnerability affects Thunderbird < 91.9.	6.5	More Details
CVE-2022-26385	In unusual circumstances, an individual thread may outlive the thread's manager during shutdown. This could have led to a use-after-free causing a potentially exploitable crash. This vulnerability affects Firefox < 98.	6.5	More Details
CVE-2022-40958	By injecting a cookie with certain special characters, an attacker on a shared subdomain which is not a secure context could set and thus overwrite cookies from a secure context, leading to session fixation and other attacks. This vulnerability affects Firefox ESR < 102.3, Thunderbird < 102.3, and Firefox < 105.	6.5	More Details
CVE-2022-40959	During iframe navigation, certain pages did not have their FeaturePolicy fully initialized leading to a bypass that leaked device permissions into untrusted subdocuments. This vulnerability affects Firefox ESR < 102.3, Thunderbird < 102.3, and Firefox < 105.	6.5	More Details
CVE-2022-34479	A malicious website that could create a popup could have resized the popup to overlay the address bar with its own content, resulting in potential user confusion or spoofing attacks. *This bug only affects Thunderbird for Linux. Other operating systems are unaffected.*. This vulnerability affects Firefox < 102, Firefox ESR < 91.11, Thunderbird < 102, and Thunderbird < 91.11.	6.5	More Details
CVE-2022-42454	Insights for Vulnerability Remediation (IVR) is vulnerable to man-in-the-middle attacks that may lead to information disclosure. This requires privileged network access.	6.4	More Details
CVE-2022-44756	Insights for Vulnerability Remediation (IVR) is vulnerable to improper input validation. This may lead to information disclosure. This requires privileged access.	6.4	More Details
CVE-2022-38655	BigFix WebUI non-master operators are missing controls that prevent them from being able to modify the relevance of fixlets or to deploy fixlets from the BES Support external site.	6.4	More Details
CVE-2022-23540	In versions `<=8.5.1` of `jsonwebtoken` library, lack of algorithm definition in the `jwt.verify()` function can lead to signature validation bypass due to defaulting to the `none` algorithm for signature verification. Users are affected if you do not specify algorithms in the `jwt.verify()` function. This issue has been fixed, please update to version 9.0.0 which removes the default support for the none algorithm in the `jwt.verify()` method. There will be no impact, if you update to version 9.0.0 and you don't need to allow for the `none` algorithm. If you need 'none' algorithm, you have to explicitly specify that in `jwt.verify()` options.	6.4	More Details
CVE-2022-4742	A vulnerability, which was classified as critical, has been found in json-pointer up to 0.6.1. Affected by this issue is the function set of the file index.js. The manipulation leads to improperly controlled modification of object prototype attributes ('prototype pollution'). The attack may be launched remotely. Upgrading to version 0.6.2 is able to address this issue. The patch is identified as 859c9984b6c407fc2d5a0a7e47c7274daa681941. It is recommended to upgrade the affected component. VDB-216794 is the identifier assigned to this vulnerability.	6.3	More Details
CVE-2022-4768	A vulnerability was found in Dropbox merou. It has been classified as critical. Affected is the function add_public_key of the file grouper/public_key.py of the component SSH Public Key Handler. The manipulation of the argument public_key_str leads to injection. It is possible to launch the attack remotely. The name of the patch is d93087973afa26bc0a2d0a5eb5c0fde748bdd107. It is recommended to apply a patch to fix this issue. VDB-216906 is the identifier assigned to this vulnerability.	6.3	More Details

CVE Number	Description	Base Score	Reference
CVE-2021-4264	A vulnerability was found in LinkedIn dustjs up to 2.x and classified as problematic. Affected by this issue is some unknown functionality. The manipulation leads to improperly controlled modification of object prototype attributes ('prototype pollution'). The attack may be launched remotely. The exploit has been disclosed to the public and may be used. Upgrading to version 3.0.0 is able to address this issue. The name of the patch is ddb6523832465d38c9d80189e9de60519ac307c3. It is recommended to upgrade the affected component. The identifier of this vulnerability is VDB-216464.	6.3	More Details
CVE-2019-25085	A vulnerability was found in GNOME gvdb. It has been classified as critical. This affects the function gvdb_table_write_contents_async of the file gvdb-builder.c. The manipulation leads to use after free. It is possible to initiate the attack remotely. The name of the patch is d83587b2a364eb9a9a53be7e6a708074e252de14. It is recommended to apply a patch to fix this issue. The identifier VDB-216789 was assigned to this vulnerability.	6.3	More Details
CVE-2020-36624	A vulnerability was found in ahorner text-helpers up to 1.0.x. It has been declared as critical. This vulnerability affects unknown code of the file lib/text_helpers/translation.rb. The manipulation of the argument link leads to use of web link to untrusted target with window.opener access. The attack can be initiated remotely. Upgrading to version 1.1.0 is able to address this issue. The name of the patch is 184b60ded0e43c985788582aca2d1e746f9405a3. It is recommended to upgrade the affected component. The identifier of this vulnerability is VDB-216520.	6.3	More Details
CVE-2022-4726	A vulnerability classified as critical was found in SourceCodester Sanitization Management System 1.0. Affected by this vulnerability is an unknown functionality of the component Admin Login. The manipulation of the argument username/password leads to sql injection. The attack can be launched remotely. The associated identifier of this vulnerability is VDB-216739.	6.3	More Details
CVE-2022-43859	IBM Navigator for i 7.3, 7.4, and 7.5 could allow an authenticated user to obtain sensitive information for an object they are authorized to but not while using this interface. By performing a UNION based SQL injection an attacker could see file permissions through this interface. IBM X-Force ID: 239304.	6.3	More Details
CVE-2022-22458	IBM Security Verify Governance, Identity Manager 10.0.1 stores user credentials in plain clear text which can be read by a remote authenticated user. IBM X-Force ID: 225009.	6.3	More Details
CVE-2021-4279	A vulnerability has been found in Starcounter-Jack JSON-Patch up to 3.1.0 and classified as problematic. This vulnerability affects unknown code. The manipulation leads to improperly controlled modification of object prototype attributes ('prototype pollution'). The attack can be initiated remotely. The exploit has been disclosed to the public and may be used. Upgrading to version 3.1.1 is able to address this issue. The name of the patch is 7ad6af41eabb2d799f698740a91284d762c955c9. It is recommended to upgrade the affected component. VDB-216778 is the identifier assigned to this vulnerability.	6.3	More Details
CVE-2020-36631	A vulnerability was found in barronwaffles dwc_network_server_emulator. It has been declared as critical. This vulnerability affects the function update_profile of the file gamespy/gs_database.py. The manipulation of the argument firstname/lastname leads to sql injection. The attack can be initiated remotely. The name of the patch is f70eb21394f75019886fbc2fb536de36161ba422. It is recommended to apply a patch to fix this issue. The identifier of this vulnerability is VDB-216772.	6.3	More Details
CVE-2020-36632	A vulnerability, which was classified as critical, was found in hughsk flat up to 5.0.0. This affects the function unflatten of the file index.js. The manipulation leads to improperly controlled modification of object prototype attributes ('prototype pollution'). It is possible to initiate the attack remotely. Upgrading to version 5.0.1 is able to address this issue. The name of the patch is 20ef0ef55dfa028caddaedbcb33efbdb04d18e13. It is recommended to upgrade the affected component. The identifier VDB-216777 was assigned to this vulnerability.	6.3	More Details
CVE-2022-4643	A vulnerability was found in docconv up to 1.2.0. It has been declared as critical. This vulnerability affects the function ConvertPDFImages of the file pdf_ocr.go. The manipulation of the argument path leads to os command injection. The attack can be initiated remotely. Upgrading to version 1.2.1 is able to address this issue. The name of the patch is b19021ade3d0b71c89d35cb00eb9e589a121faa5. It is recommended to upgrade the affected component. VDB-216502 is the identifier assigned to this vulnerability.	6.3	More Details
CVE-2022-43848	IBM AIX 7.1, 7.2, 7.3, and VIOS 3.1 could allow a non-privileged local user to exploit a vulnerability in the AIX perfstat kernel extension to cause a denial of service. IBM X-Force ID: 239169.	6.2	More Details
CVE-2022-39164	IBM AIX 7.1, 7.2, 7.3, and VIOS 3.1could allow a non-privileged local user to exploit a vulnerability in the AIX kernel to cause a denial of service. IBM X-Force ID: 235181.	6.2	More Details

CVE Number	Description	Base Score	Reference
CVE-2022-43381	IBM AIX 7.1, 7.2, 7.3, and VIOS 3.1could allow a non-privileged local user to exploit a vulnerability in the AIX SMB client to cause a denial of service. IBM X-Force ID: 238639.	6.2	More Details
CVE-2022-43380	IBM AIX 7.1, 7.2, 7.3, and VIOS 3.1 could allow a non-privileged local user to exploit a vulnerability in the AIX NFS kernel extension to cause a denial of service. IBM X-Force ID: 238640.	6.2	More Details
CVE-2022-43849	IBM AIX 7.1, 7.2, 7.3, and VIOS 3.1could allow a non-privileged local user to exploit a vulnerability in the AIX pfcdd kernel extension to cause a denial of service. IBM X-Force ID: 239170.	6.2	More Details
CVE-2022-40233	IBM AIX 7.1, 7.2, 7.3, and VIOS 3.1 could allow a non-privileged local user to exploit a vulnerability in the AIX TCP/IP kernel extension to cause a denial of service. IBM X-Force ID: 235599.	6.2	More Details
CVE-2022-39165	IBM AIX 7.1, 7.2, 7.3, and VIOS 3.1could allow a non-privileged local user to exploit a vulnerability in CAA to cause a denial of service. IBM X-Force ID: 235183.	6.2	More Details
CVE-2022-40956	When injecting an HTML base element, some requests would ignore the CSP's base-uri settings and accept the injected element's base instead. This vulnerability affects Firefox ESR < 102.3, Thunderbird < 102.3, and Firefox < 105.	6.1	More Details
CVE-2022-45413	Using the <code>S.browser_fallback_url parameter</code> parameter, an attacker could redirect a user to a URL and cause SameSite=Strict cookies to be sent. *This issue only affects Firefox for Android. Other operating systems are not affected.*. This vulnerability affects Firefox < 107.	6.1	More Details
CVE-2022-29912	Requests initiated through reader mode did not properly omit cookies with a SameSite attribute. This vulnerability affects Thunderbird < 91.9, Firefox ESR < 91.9, and Firefox < 100.	6.1	More Details
CVE-2022-40011	Cross Site Scripting (XSS) vulnerability in typora through 1.38 allows remote attackers to run arbitrary code via export from editor.	6.1	More Details
CVE-2022-4644	Open Redirect in GitHub repository ikus060/rdiffweb prior to 2.5.4.	6.1	More Details
CVE-2022-45418	If a custom mouse cursor is specified in CSS, under certain circumstances the cursor could have been drawn over the browser UI, resulting in potential user confusion or spoofing attacks. This vulnerability affects Firefox ESR < 102.5, Thunderbird < 102.5, and Firefox < 107.	6.1	More Details
CVE-2022-37310	OX App Suite through 7.10.6 allows XSS via a malicious capability to the metrics or help module, as demonstrated by a /#!!&app=io.ox/files&cap= URI.	6.1	More Details
CVE-2022-4267	The Bulk Delete Users by Email WordPress plugin through 1.2 does not sanitise and escape a parameter before outputting it back in the page, leading to a Reflected Cross-Site Scripting	6.1	More Details
CVE-2022-4647	Cross-site Scripting (XSS) - Stored in GitHub repository microweber/microweber prior to 1.3.2.	6.1	More Details
CVE-2022-45890	In Planet eStream before 6.72.10.07, a Reflected Cross-Site Scripting (XSS) vulnerability exists via any metadata filter field (e.g., search within Default.aspx with the r or fo parameter).	6.1	More Details
CVE-2022-29911	An improper implementation of the new iframe sandbox keyword <code>allow-top-navigation-by-user-activation</code> could lead to script execution without <code>allow-scripts</code> being present. This vulnerability affects Thunderbird < 91.9, Firefox ESR < 91.9, and Firefox < 100.	6.1	More Details

CVE Number	Description	Base Score	Reference
CVE-2022-29910	When closed or sent to the background, Firefox for Android would not properly record and persist HSTS settings. *Note: This issue only affected Firefox for Android. Other operating systems are unaffected.*. This vulnerability affects Firefox < 100.	6.1	More Details
CVE-2022-4227	The Booster for WooCommerce WordPress plugin before 5.6.3, Booster Plus for WooCommerce WordPress plugin before 6.0.0, Booster Elite for WooCommerce WordPress plugin before 6.0.0 do not escape some URLs and parameters before outputting them back in attributes, leading to Reflected Cross-Site Scripting	6.1	More Details
CVE-2022-34475	SVG <code><use></code> tags that referenced a same-origin document could have resulted in script execution if attacker input was sanitized via the HTML Sanitizer API. This would have required the attacker to reference a same-origin JavaScript file containing the script to be executed. This vulnerability affects Firefox < 102.	6.1	More Details
CVE-2022-37309	OX App Suite through 7.10.6 allows XSS via script code within a contact that has an e-mail address but lacks a name.	6.1	More Details
CVE-2022-37308	OX App Suite through 7.10.6 allows XSS via HTML in text/plain e-mail messages.	6.1	More Details
CVE-2022-34473	The HTML Sanitizer should have sanitized the <code>href</code> attribute of SVG <code><use></code> tags; however it incorrectly did not sanitize <code>xlink:href</code> attributes. This vulnerability affects Firefox < 102.	6.1	More Details
CVE-2021-30134	php-mod/curl (a wrapper of the PHP cURL extension) before 2.3.2 allows XSS via the post_file_path_upload.php key parameter and the POST data to post_multidimensional.php.	6.1	More Details
CVE-2022-45411	Cross-Site Tracing occurs when a server will echo a request back via the Trace method, allowing an XSS attack to access to authorization headers and cookies inaccessible to JavaScript (such as cookies protected by HTTPOnly). To mitigate this attack, browsers placed limits on <code>fetch()</code> and XMLHttpRequest; however some webservers have implemented non-standard headers such as <code>X-Http-Method-Override</code> that override the HTTP method, and made this attack possible again. Thunderbird has applied the same mitigations to the use of this and similar headers. This vulnerability affects Firefox ESR < 102.5, Thunderbird < 102.5, and Firefox < 107.	6.1	More Details
CVE-2022-47928	In MISP before 2.4.167, there is XSS in the template file uploads in app/View/Templates/upload_file.ctp.	6.1	More Details
CVE-2022-36316	When using the Performance API, an attacker was able to notice subtle differences between PerformanceEntries and thus learn whether the target URL had been subject to a redirect. This vulnerability affects Firefox < 103.	6.1	More Details
CVE-2022-46095	Sourcecodester Covid-19 Directory on Vaccination System 1.0 was discovered to contain a Cross-Site Scripting (XSS) vulnerability via verification.php because the program does not verify the txtvaccinationID parameter.	6.1	More Details
CVE-2022-46096	A Cross site scripting (XSS) vulnerability in Sourcecodester Online Covid-19 Directory on Vaccination System v1.0 allows attackers to execute arbitrary code via the txtfullname parameter or txtphone parameter to register.php without logging in.	6.1	More Details
CVE-2022-40841	A cross-site scripting (XSS) vulnerability in NdkAdvancedCustomizationFields v3.5.0 allows attackers to execute arbitrary web scripts or HTML via a crafted payloads injected into the "htmlNodes" parameter.	6.1	More Details
CVE-2022-4617	Cross-site Scripting (XSS) - Reflected in GitHub repository microweber/microweber prior to 1.3.2.	6.1	More Details
CVE-2022-4720	Open Redirect in GitHub repository ikus060/rdiffweb prior to 2.5.5.	6.1	More Details
CVE-2022-31469	OX App Suite through 7.10.6 allows XSS via a deep link, as demonstrated by class="deep-link-app" for a /#!!&app=%2e./ URI.	6.1	More Details

CVE Number	Description	Base Score	Reference
CVE-2022-34474	Even when an iframe was sandboxed with <code>allow-top-navigation-by-user-activation</code>, if it received a redirect header to an external protocol the browser would process the redirect and prompt the user as appropriate. This vulnerability affects Firefox < 102.	6.1	More Details
CVE-2022-36664	Password Manager for IIS 2.0 has a cross-site scripting (XSS) vulnerability via the /isapi/PasswordManager.dll ResultURL parameter.	6.1	More Details
CVE-2022-37307	OX App Suite through 7.10.6 allows XSS via XHTML CDATA for a snippet, as demonstrated by the onerror attribute of an IMG element within an e-mail signature.	6.1	More Details
CVE-2022-45434	Some Dahua software products have a vulnerability of unauthenticated un-throttled ICMP requests on remote DSS Server. After bypassing the firewall access control policy, by sending a specific crafted packet to the vulnerable interface, an attacker could exploit the victim server to launch ICMP request attack to the designated target host.	5.9	More Details
CVE-2022-43596	An information disclosure vulnerability exists in the IFFOutput channel interleaving functionality of OpenImageIO Project OpenImageIO v2.4.4.2. A specially crafted ImageOutput Object can lead to leaked heap data. An attacker can provide malicious input to trigger this vulnerability.	5.9	More Details
CVE-2022-43593	A denial of service vulnerability exists in the DPXOutput::close() functionality of OpenImageIO Project OpenImageIO v2.4.4.2. A specially crafted ImageOutput Object can lead to null pointer dereference. An attacker can provide malicious input to trigger this vulnerability.	5.9	More Details
CVE-2022-35646	IBM Security Verify Governance, Identity Manager 10.0.1 software component could allow an authenticated user to modify or cancel any other user's access request using man-in-the-middle techniques. IBM X-Force ID: 231096.	5.9	More Details
CVE-2022-22461	IBM Security Verify Governance, Identity Manager 10.0.1 uses weaker than expected cryptographic algorithms that could allow an attacker to decrypt highly sensitive information. IBM X-Force ID: 225007.	5.9	More Details
CVE-2022-43592	An information disclosure vulnerability exists in the DPXOutput::close() functionality of OpenImageIO Project OpenImageIO v2.4.4.2. A specially crafted ImageOutput Object can lead to leaked heap data. An attacker can provide malicious input to trigger this vulnerability.	5.9	More Details
CVE-2022-23539	Versions `<=8.5.1` of `jsonwebtoken` library could be misconfigured so that legacy, insecure key types are used for signature verification. For example, DSA keys could be used with the RS256 algorithm. You are affected if you are using an algorithm and a key type other than a combination listed in the GitHub Security Advisory as unaffected. This issue has been fixed, please update to version 9.0.0. This version validates for asymmetric key type and algorithm combinations. Please refer to the above mentioned algorithm / key type combinations for the valid secure configuration. After updating to version 9.0.0, if you still intend to continue with signing or verifying tokens using invalid key type/algorithm value combinations, you'll need to set the `allowInvalidAsymmetricKeyTypes` option to `true` in the `sign()` and/or `verify()` functions.	5.9	More Details
CVE-2022-43594	Multiple denial of service vulnerabilities exist in the image output closing functionality of OpenImageIO Project OpenImageIO v2.4.4.2. Specially crafted ImageOutput Objects can lead to multiple null pointer dereferences. An attacker can provide malicious multiple inputs to trigger these vulnerabilities.This vulnerability applies to writing .bmp files.	5.9	More Details
CVE-2022-43595	Multiple denial of service vulnerabilities exist in the image output closing functionality of OpenImageIO Project OpenImageIO v2.4.4.2. Specially crafted ImageOutput Objects can lead to multiple null pointer dereferences. An attacker can provide malicious multiple inputs to trigger these vulnerabilities.This vulnerability applies to writing .fits files.	5.9	More Details
CVE-2022-43603	A denial of service vulnerability exists in the ZfileOutput::close() functionality of OpenImageIO Project OpenImageIO v2.4.4.2. A specially crafted ImageOutput Object can lead to denial of service. An attacker can provide a malicious file to trigger this vulnerability.	5.9	More Details
CVE-2022-22746	A race condition could have allowed bypassing the fullscreen notification which could have lead to a fullscreen window spoof being unnoticed. *This bug only affects Firefox for Windows. Other operating systems are unaffected.*. This vulnerability affects Firefox ESR < 91.5, Firefox < 96, and Thunderbird < 91.5.	5.9	More Details
CVE-2022-40897	Python Packaging Authority (PyPA) setuptools before 65.5.1 allows remote attackers to cause a denial of service via HTML in a crafted package or custom PackageIndex page. There is a Regular Expression Denial of Service (ReDoS) in package_index.py.	5.9	More Details

CVE Number	Description	Base Score	Reference
CVE-2022-4639	A vulnerability, which was classified as critical, has been found in sslh. This issue affects the function hexdump of the file probe.c of the component Packet Dumping Handler. The manipulation of the argument msg_info leads to format string. The attack may be initiated remotely. The name of the patch is b19f8a6046b080e4c2e28354a58556bb26040c6f. It is recommended to apply a patch to fix this issue. The identifier VDB-216497 was assigned to this vulnerability.	5.6	More Details
CVE-2021-4290	A vulnerability was found in DHBW Fallstudie. It has been declared as critical. Affected by this vulnerability is an unknown functionality of the file app/config/passport.js of the component Login. The manipulation of the argument id/email leads to sql injection. The name of the patch is 5c13c6a972ef4c07c5f35b417916e0598af9e123. It is recommended to apply a patch to fix this issue. The associated identifier of this vulnerability is VDB-216907.	5.5	More Details
CVE-2022-4662	A flaw incorrect access control in the Linux kernel USB core subsystem was found in the way user attaches usb device. A local user could use this flaw to crash the system.	5.5	More Details
CVE-2021-4278	A vulnerability classified as problematic has been found in cronvel tree-kit up to 0.6.x. This affects an unknown part. The manipulation leads to improperly controlled modification of object prototype attributes ('prototype pollution'). Upgrading to version 0.7.0 is able to address this issue. The name of the patch is a63f559c50d70e8cb2eaae670dec25d1dbc4afcd. It is recommended to upgrade the affected component. The identifier VDB-216765 was assigned to this vulnerability.	5.5	More Details
CVE-2021-4235	Due to unbounded alias chasing, a maliciously crafted YAML file can cause the system to consume significant system resources. If parsing user input, this may be used as a denial of service vector.	5.5	More Details
CVE-2020-36630	A vulnerability was found in FreePBX cdr 14.0. It has been classified as critical. This affects the function ajaxHandler of the file ucp/Cdr.class.php. The manipulation of the argument limit/offset leads to sql injection. Upgrading to version 14.0.5.21 is able to address this issue. The name of the patch is f1a9eea2dfff30fb99d825bac194a676a82b9ec8. It is recommended to upgrade the affected component. The associated identifier of this vulnerability is VDB-216771.	5.5	More Details
CVE-2022-4725	A vulnerability was found in AWS SDK 2.59.0. It has been rated as critical. This issue affects the function XpathUtils of the file aws-android-sdk-core/src/main/java/com/amazonaws/util/XpathUtils.java of the component XML Parser. The manipulation leads to server-side request forgery. Upgrading to version 2.59.1 is able to address this issue. The name of the patch is c3e6d69422e1f0c80fe53f2d757b8df97619af2b. It is recommended to upgrade the affected component. The identifier VDB-216737 was assigned to this vulnerability.	5.5	More Details
CVE-2020-36629	A vulnerability classified as critical was found in SimbCo httpster. This vulnerability affects the function fs.realpathSync of the file src/server.coffee. The manipulation leads to path traversal. The exploit has been disclosed to the public and may be used. The name of the patch is d3055b3e30b40b65d30c5a06d6e053dffa7f35d0. It is recommended to apply a patch to fix this issue. The identifier of this vulnerability is VDB-216748.	5.5	More Details
CVE-2020-36628	A vulnerability classified as critical has been found in Calsign APDE. This affects the function handleExtract of the file APDE/src/main/java/com/calsignlabs/apde/build/dag/CopyBuildTask.java of the component ZIP File Handler. The manipulation leads to path traversal. Upgrading to version 0.5.2-pre2-alpha is able to address this issue. It is recommended to upgrade the affected component. The associated identifier of this vulnerability is VDB-216747.	5.5	More Details
CVE-2020-36627	A vulnerability was found in Macaron i18n. It has been declared as problematic. Affected by this vulnerability is an unknown functionality of the file i18n.go. The manipulation leads to open redirect. The attack can be launched remotely. Upgrading to version 0.5.0 is able to address this issue. The name of the patch is 329b0c4844cc16a5a253c011b55180598e707735. It is recommended to upgrade the affected component. The identifier VDB-216745 was assigned to this vulnerability.	5.5	More Details
CVE-2020-36626	A vulnerability classified as critical has been found in Modern Tribe Panel Builder Plugin. Affected is the function add_post_content_filtered_to_search_sql of the file ModularContent/SearchFilter.php. The manipulation leads to sql injection. It is possible to launch the attack remotely. The exploit has been disclosed to the public and may be used. The name of the patch is 4528d4f855dbbf24e9fc12a162fda84ce3bedc2f. It is recommended to apply a patch to fix this issue. VDB-216738 is the identifier assigned to this vulnerability.	5.5	More Details
CVE-2022-47946	An issue was discovered in the Linux kernel 5.10.x before 5.10.155. A use-after-free in io_sqpoll_wait_sq in fs/io_uring.c allows an attacker to crash the kernel, resulting in denial of service. finish_wait can be skipped. An attack can occur in some situations by forking a process and then quickly terminating it. NOTE: later kernel versions, such as the 5.15 longterm series, substantially changed the implementation of io_sqpoll_wait_sq.	5.5	More Details

CVE Number	Description	Base Score	Reference
CVE-2021-43395	An issue was discovered in illumos before f859e7171bb5db34321e45585839c6c3200ebb90, OmniOS Community Edition r151038, OpenIndiana Hipster 2021.04, and SmartOS 20210923. A local unprivileged user can cause a deadlock and kernel panic via crafted rename and rmdir calls on tmpfs filesystems. Oracle Solaris 10 and 11 is also affected.	5.5	More Details
CVE-2022-4748	A vulnerability was found in FlatPress. It has been classified as critical. This affects the function doItemActions of the file fp-plugins/mediamanager/panels/panel.mediamanager.file.php of the component File Delete Handler. The manipulation of the argument deletefile leads to path traversal. The name of the patch is 5d5c7f6d8f072d14926fc2c3a97cdd763802f170. It is recommended to apply a patch to fix this issue. The identifier VDB-216861 was assigned to this vulnerability.	5.5	More Details
CVE-2022-4698	The ProfilePress plugin for WordPress is vulnerable to Stored Cross-Site Scripting via several form fields in versions up to, and including, 4.5.0 due to insufficient input sanitization and output escaping. This makes it possible for authenticated attackers, with administrator-level permissions and above, to inject arbitrary web scripts in pages that will execute whenever a user accesses an injected page. This only affects multi-site installations and installations where unfiltered_html has been disabled.	5.5	More Details
CVE-2022-3266	An out-of-bounds read can occur when decoding H264 video. This results in a potentially exploitable crash. This vulnerability affects Firefox ESR < 102.3, Thunderbird < 102.3, and Firefox < 105.	5.5	More Details
CVE-2022-4697	The ProfilePress plugin for WordPress is vulnerable to Stored Cross-Site Scripting via the 'wp_user_cover_default_image_url' parameter in versions up to, and including, 4.5.0 due to insufficient input sanitization and output escaping. This makes it possible for authenticated attackers, with administrator-level permissions and above, to inject arbitrary web scripts in pages that will execute whenever a user accesses an injected page. This only affects multi-site installations and installations where unfiltered_html has been disabled.	5.5	More Details
CVE-2022-36314	When opening a Windows shortcut from the local filesystem, an attacker could supply a remote path that would lead to unexpected network requests from the operating system. This bug only affects Firefox for Windows. Other operating systems are unaffected.*. This vulnerability affects Firefox ESR < 102.1, Firefox < 103, and Thunderbird < 102.1.	5.5	More Details
CVE-2022-41684	A heap out of bounds read vulnerability exists in the OpenImageIO master-branch-9aeece7a when parsing the image file directory part of a PSD image file. A specially-crafted .psd file can cause a read of arbitrary memory address which can lead to denial of service. An attacker can provide a malicious file to trigger this vulnerability.	5.5	More Details
CVE-2022-4691	Cross-site Scripting (XSS) - Stored in GitHub repository usememos/memos prior to 0.9.0.	5.4	More Details
CVE-2022-4694	Cross-site Scripting (XSS) - Stored in GitHub repository usememos/memos prior to 0.9.0.	5.4	More Details
CVE-2022-29852	OX App Suite through 8.2 allows XSS because BMFreehand10 and image/x-freehand are not blocked.	5.4	More Details
CVE-2022-4721	Failure to Sanitize Special Elements into a Different Plane (Special Element Injection) in GitHub repository ikus060/rdiffweb prior to 2.5.5.	5.4	More Details
CVE-2021-44855	An issue was discovered in MediaWiki before 1.35.5, 1.36.x before 1.36.3, and 1.37.x before 1.37.1. There is Blind Stored XSS via a URL to the Upload Image feature.	5.4	More Details
CVE-2022-28286	Due to a layout change, iframe contents could have been rendered outside of its border. This could have led to user confusion or spoofing attacks. This vulnerability affects Thunderbird < 91.8, Firefox < 99, and Firefox ESR < 91.8.	5.4	More Details
CVE-2022-29853	OX App Suite through 8.2 allows XSS via a certain complex hierarchy that forces use of Show Entire Message for a huge HTML e-mail message.	5.4	More Details

CVE Number	Description	Base Score	Reference
CVE-2022-4695	Cross-site Scripting (XSS) - Stored in GitHub repository usememos/memos prior to 0.9.0.	5.4	More Details
CVE-2022-3794	The Jeg Elementor Kit plugin for WordPress is vulnerable to authorization bypass in various AJAX actions in versions up to, and including, 2.5.6. Authenticated users can use an easily available nonce value to create header templates and make additional changes to the site, as the plugin does not use capability checks for this purpose.	5.4	More Details
CVE-2022-44380	Snipe-IT before 6.0.14 is vulnerable to Cross Site Scripting (XSS) for View Assigned Assets.	5.4	More Details
CVE-2022-44510	Adobe Experience Manager version 6.5.14 (and earlier) is affected by a reflected Cross-Site Scripting (XSS) vulnerability. If a low-privileged attacker is able to convince a victim to visit a URL referencing a vulnerable page, malicious JavaScript content may be executed within the context of the victim's browser.	5.4	More Details
CVE-2022-4692	Cross-site Scripting (XSS) - Stored in GitHub repository usememos/memos prior to 0.9.0.	5.4	More Details
CVE-2022-45892	In Planet eStream before 6.72.10.07, multiple Stored Cross-Site Scripting (XSS) vulnerabilities exist: Disclaimer, Search Function, Comments, Batch editing tool, Content Creation, Related Media, Create new user, and Change Username.	5.4	More Details
CVE-2022-47968	Heimdall Application Dashboard through 2.5.4 allows reflected and stored XSS via "Application name" to the "Add application" page. The stored XSS will be triggered in the "Application list" page.	5.4	More Details
CVE-2021-43657	A Stored Cross-site scripting (XSS) vulnerability via MAster.php in Sourcecodetester Simple Client Management System (SCMS) 1.0 allows remote attackers to inject arbitrary web script or HTML via the vulnerable input fields.	5.4	More Details
CVE-2022-43271	Inhabit Systems Pty Ltd Move CRM version 4, build 260 was discovered to contain a cross-site scripting (XSS) vulnerability via the User profile component.	5.4	More Details
CVE-2022-44012	An issue was discovered in /DS/LM_API/api/SelectionService/InsertQueryWithActiveRelationsReturnId in Simmeth Lieferantenmanager before 5.6. An attacker can execute JavaScript code in the browser of the victim if a site is loaded. The victim's encrypted password can be stolen and most likely be decrypted.	5.4	More Details
CVE-2022-47524	F-Secure SAFE Browser 19.1 before 19.2 for Android allows an IDN homograph attack.	5.4	More Details
CVE-2022-1197	When importing a revoked key that specified key compromise as the revocation reason, Thunderbird did not update the existing copy of the key that was not yet revoked, and the existing key was kept as non-revoked. Revocation statements that used another revocation reason, or that didn't specify a revocation reason, were unaffected. This vulnerability affects Thunderbird < 91.8.	5.4	More Details
CVE-2022-43543	KDDI +Message App, NTT DOCOMO +Message App, and SoftBank +Message App contain a vulnerability caused by improper handling of Unicode control characters. +Message App displays text unprocessed, even when control characters are contained, and the text is shown based on Unicode control character's specifications. Therefore, a crafted text may display misleading web links. As a result, a spoofed URL may be displayed and phishing attacks may be conducted. Affected products and versions are as follows: KDDI +Message App for Android prior to version 3.9.2 and +Message App for iOS prior to version 3.9.4, NTT DOCOMO +Message App for Android prior to version 54.49.0500 and +Message App for iOS prior to version 3.9.4, and SoftBank +Message App for Android prior to version 12.9.5 and +Message App for iOS prior to version 3.9.4	5.4	More Details
CVE-2022-25929	The package smoothie from 1.31.0 and before 1.36.1 are vulnerable to Cross-site Scripting (XSS) due to improper user input sanitization in strokeStyle and tooltipLabel properties. Exploiting this vulnerability is possible when the user can control these properties.	5.4	More Details
CVE-2022-4690	Cross-site Scripting (XSS) - Stored in GitHub repository usememos/memos prior to 0.9.0.	5.4	More Details

CVE Number	Description	Base Score	Reference
CVE-2022-3189	Dataprobe iBoot-PDU FW versions prior to 1.42.06162022 contain a vulnerability where a specially crafted PHP script could use parameters from a HTTP request to create a URL capable of changing the host parameter. The changed host parameter in the HTTP could point to another host that will send a request to the host or IP specified in the changed host parameter.	5.3	More Details
CVE-2022-41767	An issue was discovered in MediaWiki before 1.35.8, 1.36.x and 1.37.x before 1.37.5, and 1.38.x before 1.38.3. When changes made by an IP address are reassigned to a user (using reassignEdits.php), the changes will still be attributed to the IP address on Special:Contributions when doing a range lookup.	5.3	More Details
CVE-2022-41765	An issue was discovered in MediaWiki before 1.35.8, 1.36.x and 1.37.x before 1.37.5, and 1.38.x before 1.38.3. HTMLUserTextField exposes the existence of hidden users.	5.3	More Details
CVE-2022-22449	IBM Security Verify Governance, Identity Manager 10.01 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: 224915.	5.3	More Details
CVE-2019-9011	In Pilz PMC programming tool 3.x before 3.5.17 (based on CODESYS Development System), an attacker can identify valid usernames.	5.3	More Details
CVE-2022-3188	Dataprobe iBoot-PDU FW versions prior to 1.42.06162022 contain a vulnerability where unauthenticated users could open PHP index pages without authentication and download the history file from the device; the history file includes the latest actions completed by specific users.	5.3	More Details
CVE-2022-36318	When visiting directory listings for `chrome://` URLs as source text, some parameters were reflected. This vulnerability affects Firefox ESR < 102.1, Firefox ESR < 91.12, Firefox < 103, Thunderbird < 102.1, and Thunderbird < 91.12.	5.3	More Details
CVE-2019-19030	Cloud Native Computing Foundation Harbor before 1.10.3 and 2.x before 2.0.1 allows resource enumeration because unauthenticated API calls reveal (via the HTTP status code) whether a resource exists.	5.3	More Details
CVE-2022-3185	Dataprobe iBoot-PDU FW versions prior to 1.42.06162022 contain a vulnerability where the affected product exposes sensitive data concerning the device.	5.3	More Details
CVE-2022-3187	Dataprobe iBoot-PDU FW versions prior to 1.42.06162022 contain a vulnerability where certain PHP pages only validate when a valid connection is established with the database. However, these PHP pages do not verify the validity of a user. Attackers could leverage this lack of verification to read the state of outlets.	5.3	More Details
CVE-2019-14802	HashiCorp Nomad 0.5.0 through 0.9.4 (fixed in 0.9.5) reveals unintended environment variables to the rendering task during template rendering, aka GHSA-6hv3-7c34-4hx8. This applies to nomad/client/allocrunner/taskrunner/template.	5.3	More Details
CVE-2019-25087	A vulnerability was found in RamseyK httpserver. It has been rated as critical. This issue affects the function ResourceHost::getResource of the file src/ResourceHost.cpp of the component URI Handler. The manipulation of the argument uri leads to path traversal: '../filedir'. The attack may be initiated remotely. The name of the patch is 1a0de56e4dafff9c2f9c8f6b130a764f7a50df52. It is recommended to apply a patch to fix this issue. The associated identifier of this vulnerability is VDB-216863.	5.3	More Details
CVE-2022-41697	A user enumeration vulnerability exists in the login functionality of Ghost Foundation Ghost 5.9.4. A specially-crafted HTTP request can lead to a disclosure of sensitive information. An attacker can send a series of HTTP requests to trigger this vulnerability.	5.3	More Details
CVE-2021-44856	An issue was discovered in MediaWiki before 1.35.5, 1.36.x before 1.36.3, and 1.37.x before 1.37.1. A title blocked by AbuseFilter can be created via Special:ChangeContentModel due to the mishandling of the EditFilterMergedContent hook return value.	5.3	More Details
CVE-2022-37311	OX App Suite through 7.10.6 has Uncontrolled Resource Consumption via a large location request parameter to the redirect servlet.	5.3	More Details
CVE-2022-44381	Snipe-IT through 6.0.14 allows attackers to check whether a user account exists because of response variations in a /password/reset request.	5.3	More Details

CVE Number	Description	Base Score	Reference
CVE-2022-38546	A DNS misconfiguration was found in Zyxel NBG7510 firmware versions prior to V1.00(ABZY.3)C0, which could allow an unauthenticated attacker to access the DNS server when the device is switched to the AP mode.	5.3	More Details
CVE-2022-23513	Pi-Hole is a network-wide ad blocking via your own Linux hardware, AdminLTE is a Pi-hole Dashboard for stats and more. In case of an attack, the threat actor will obtain the ability to perform an unauthorized query for blocked domains on `queryads` endpoint. In the case of application, this vulnerability exists because of a lack of validation in code on a root server path: `/admin/scripts/pi-hole/phpqueryads.php.` Potential threat actor(s) are able to perform an unauthorized query search in blocked domain lists. This could lead to the disclosure for any victims' personal blacklists.	5.3	More Details
CVE-2022-4630	Sensitive Cookie Without 'HttpOnly' Flag in GitHub repository lirantal/daloradius prior to master.	5.3	More Details
CVE-2022-45432	Some Dahua software products have a vulnerability of unauthenticated search for devices. After bypassing the firewall access control policy, by sending a specific crafted packet to the vulnerable interface, an attacker could unauthenticated search for devices in range of IPs from remote DSS Server.	5.3	More Details
CVE-2022-45424	Some Dahua software products have a vulnerability of unauthenticated request of AES crypto key. An attacker can obtain the AES crypto key by sending a specific crafted packet to the vulnerable interface.	5.3	More Details
CVE-2022-36354	A heap out-of-bounds read vulnerability exists in the RLA format parser of OpenImageIO master-branch-9aeece7a and v2.3.19.0. More specifically, in the way run-length encoded byte spans are handled. A malformed RLA file can lead to an out-of-bounds read of heap metadata which can result in sensitive information leak. An attacker can provide a malicious file to trigger this vulnerability.	5.3	More Details
CVE-2022-23551	aad-pod-identity assigns Azure Active Directory identities to Kubernetes applications and has now been deprecated as of 24 October 2022. The NMI component in AAD Pod Identity intercepts and validates token requests based on regex. In this case, a token request made with backslash in the request (example: `/metadata/identity\oauth2\token/`) would bypass the NMI validation and be sent to IMDS allowing a pod in the cluster to access identities that it shouldn't have access to. This issue has been fixed and has been included in AAD Pod Identity release version 1.8.13. If using the AKS pod-managed identities add-on, no action is required. The clusters should now be running the version 1.8.13 release.	5.3	More Details
CVE-2022-22457	IBM Security Verify Governance, Identity Manager 10.0.1 stores sensitive information including user credentials in plain clear text which can be read by a local privileged user. IBM X-Force ID: 225007.	5.3	More Details
CVE-2022-44565	An improper access validation vulnerability exists in airMAX AC <8.7.11, airFiber 60/LR <2.6.2, airFiber 60 XG/HD <v1.0.0 and airFiber GBE <1.4.1 that allows a malicious actor to retrieve status and usage data from the UISP device.	5.3	More Details
CVE-2022-37313	OX App Suite through 7.10.6 allows SSRF because the anti-SSRF protection mechanism only checks the first DNS AA or AAAA record.	5.3	More Details
CVE-2022-37312	OX App Suite through 7.10.6 has Uncontrolled Resource Consumption via a large request body containing a redirect URL to the deferrer servlet.	5.3	More Details
CVE-2021-35952	fastrack Reflex 2.0 W307S_REFLEX_v90.89 Activity Tracker allows a Remote attacker to change the time, date, and month via Bluetooth LE Characteristics on handle 0x0017.	5.3	More Details
CVE-2021-44854	An issue was discovered in MediaWiki before 1.35.5, 1.36.x before 1.36.3, and 1.37.x before 1.37.1. The REST API publicly caches results from private wikis.	5.3	More Details
CVE-2022-25948	The package liquidjs before 10.0.0 are vulnerable to Information Exposure when ownPropertyOnly parameter is set to False, which results in leaking properties of a prototype. Workaround For versions 9.34.0 and higher, an option to disable this functionality is provided.	5.3	More Details

CVE Number	Description	Base Score	Reference
CVE-2022-47896	In JetBrains IntelliJ IDEA before 2022.3.1 code Templates were vulnerable to SSTI attacks.	5.0	More Details
CVE-2022-23541	jsonwebtoken is an implementation of JSON Web Tokens. Versions `<= 8.5.1` of `jsonwebtoken` library can be misconfigured so that passing a poorly implemented key retrieval function referring to the `secretOrPublicKey` argument from the readme link will result in incorrect verification of tokens. There is a possibility of using a different algorithm and key combination in verification, other than the one that was used to sign the tokens. Specifically, tokens signed with an asymmetric public key could be verified with a symmetric HS256 algorithm. This can lead to successful validation of forged tokens. If your application is supporting usage of both symmetric key and asymmetric key in jwt.verify() implementation with the same key retrieval function. This issue has been patched, please update to version 9.0.0.	5.0	More Details
CVE-2021-4287	A vulnerability, which was classified as problematic, was found in ReFirm Labs binwalk up to 2.3.2. Affected is an unknown function of the file src/binwalk/modules/extractor.py of the component Archive Extraction Handler. The manipulation leads to symlink following. It is possible to launch the attack remotely. Upgrading to version 2.3.3 is able to address this issue. The name of the patch is fa0c0bd59b8588814756942fe4cb5452e76c1dcd. It is recommended to upgrade the affected component. The identifier of this vulnerability is VDB-216876.	5.0	More Details
CVE-2022-4154	The Contest Gallery Pro WordPress plugin before 19.1.5 does not escape the wp_user_id GET parameter before concatenating it to an SQL query in management-show-user.php. This may allow malicious users with at administrator privileges (i.e. on multisite WordPress configurations) to leak sensitive information from the site's database.	4.9	More Details
CVE-2022-4157	The Contest Gallery WordPress plugin before 19.1.5.1, Contest Gallery Pro WordPress plugin before 19.1.5.1 do not escape the cg_option_id POST parameter before concatenating it to an SQL query in export-votes-all.php. This may allow malicious users with administrator privileges (i.e. on multisite WordPress configurations) to leak sensitive information from the site's database.	4.9	More Details
CVE-2022-4155	The Contest Gallery WordPress plugin before 19.1.5.1, Contest Gallery Pro WordPress plugin before 19.1.5.1 do not escape the wp_user_id GET parameter before concatenating it to an SQL query in management-show-user.php. This may allow malicious users with administrator privileges (i.e. on multisite WordPress configurations) to leak sensitive information from the site's database.	4.9	More Details
CVE-2022-3835	The Kwayy HTML Sitemap WordPress plugin before 4.0 does not sanitise and escape some of its settings, which could allow high privilege users such as admin to perform Stored Cross-Site Scripting attacks even when the unfiltered_html capability is disallowed (for example in multisite setup).	4.8	More Details
CVE-2022-4042	The Paytium: Mollie payment forms & donations WordPress plugin before 4.3.7 does not sanitise and escape some of its settings, which could allow high privilege users such as admin to perform Stored Cross-Site Scripting attacks even when the unfiltered_html capability is disallowed (for example in multisite setup).	4.8	More Details
CVE-2022-44449	Stored cross-site scripting vulnerability in Zenphoto versions prior to 1.6 allows remote a remote authenticated attacker with an administrative privilege to inject an arbitrary script.	4.8	More Details
CVE-2022-4242	The WP Google Review Slider WordPress plugin before 11.6 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-2022-4243	The ImageInject WordPress plugin through 1.17 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-2022-4733	Cross-site Scripting (XSS) - Stored in GitHub repository openemr/openemr prior to 7.0.0.2.	4.8	More Details
CVE-2022-4197	The Sliderby10Web WordPress plugin before 1.2.53 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-2022-4226	The Simple Basic Contact Form WordPress plugin before 20221201 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-2022-3840	The Login for Google Apps WordPress plugin before 3.4.5 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-2022-4110	The Eventify™ WordPress plugin through 2.1 does not sanitise and escape some of its settings, which could allow high privilege users such as admin to perform Stored Cross-Site Scripting attacks even when the unfiltered_html capability is disallowed (for example in multisite setup).	4.8	More Details
CVE-2022-47895	In JetBrains IntelliJ IDEA before 2022.3.1 the "Validate JSP File" action used the HTTP protocol to download required JAR files.	4.7	More Details
CVE-2022-24120	Certain General Electric Renewable Energy products store cleartext credentials in flash memory. This affects iNET and iNET II before 8.3.0.	4.6	More Details
CVE-2021-4281	A vulnerability was found in Brave UX for-the-badge and classified as critical. Affected by this issue is some unknown functionality of the file .github/workflows/combine-prs.yml. The manipulation leads to os command injection. The name of the patch is 55b5a234c0fab935df5fb08365bc8fe9c37cf46b. It is recommended to apply a patch to fix this issue. VDB-216842 is the identifier assigned to this vulnerability.	4.6	More Details
CVE-2022-4772	A vulnerability was found in Widoco and classified as critical. Affected by this issue is the function unZipIt of the file src/main/java/widoco/WidocoUtils.java. The manipulation leads to path traversal. It is possible to launch the attack on the local host. The name of the patch is f2279b76827f32190adfa9bd5229b7d5a147fa92. It is recommended to apply a patch to fix this issue. VDB-216914 is the identifier assigned to this vulnerability.	4.5	More Details
CVE-2020-36625	A vulnerability was found in destiny.gg chat. It has been rated as problematic. This issue affects the function websocket.Upgrader of the file main.go. The manipulation leads to cross-site request forgery. The attack may be initiated remotely. The name of the patch is bebd256fc3063111fb4503ca25e005ebf6e73780. It is recommended to apply a patch to fix this issue. The identifier VDB-216521 was assigned to this vulnerability. NOTE: This vulnerability only affects products that are no longer supported by the maintainer.	4.3	More Details
CVE-2022-38474	A website that had permission to access the microphone could record audio without the audio notification being shown. This bug does not allow the attacker to bypass the permission prompt - it only affects the notification shown once permission has been granted. *This bug only affects Firefox for Android. Other operating systems are unaffected.*. This vulnerability affects Firefox < 104.	4.3	More Details
CVE-2020-36633	A vulnerability was found in moodle-block_sitenews 1.0. It has been classified as problematic. This affects the function get_content of the file block_sitenews.php. The manipulation leads to cross-site request forgery. It is possible to initiate the attack remotely. Upgrading to version 1.1 is able to address this issue. The name of the patch is cd18d8b1afe464ae6626832496f4e070bac4c58f. It is recommended to upgrade the affected component. The associated identifier of this vulnerability is VDB-216879.	4.3	More Details
CVE-2022-4766	A vulnerability was found in dolibarr_project_timesheet up to 4.5.5. It has been declared as problematic. This vulnerability affects unknown code of the component Form Handler. The manipulation leads to cross-site request forgery. The attack can be initiated remotely. Upgrading to version 4.5.6.a is able to address this issue. The name of the patch is 082282e9dab43963e6c8f03cfaddd7921de377f4. It is recommended to upgrade the affected component. The identifier of this vulnerability is VDB-216880.	4.3	More Details
CVE-2022-45417	Service Workers did not detect Private Browsing Mode correctly in all cases, which could have led to Service Workers being written to disk for websites visited in Private Browsing Mode. This would not have persisted them in a state where they would run again, but it would have leaked Private Browsing Mode details to disk. This vulnerability affects Firefox < 107.	4.3	More Details
CVE-2022-46877	By confusing the browser, the fullscreen notification could have been delayed or suppressed, resulting in potential user confusion or spoofing attacks. This vulnerability affects Firefox < 108.	4.3	More Details
CVE-2022-43857	IBM Navigator for i 7.3, 7.4 and 7.5 could allow an authenticated user to access IBM Navigator for i log files they are authorized to but not while using this interface. The remote authenticated user can bypass the interface checks and download log files by modifying servlet filter. IBM X-Force ID: 239301.	4.3	More Details
CVE-2022-43858	IBM Navigator for i 7.3, 7.4, and 7.5 could allow an authenticated user to access the file system and download files they are authorized to but not while using this interface. The remote authenticated user can bypass the interface checks by modifying a parameter thereby gaining access to their files through this interface. IBM X-Force ID: 239303.	4.3	More Details

CVE Number	Description	Base Score	Reference
CVE-2021-4275	A vulnerability, which was classified as problematic, was found in katlings pyambic-pentameter. Affected is an unknown function. The manipulation leads to cross-site request forgery. It is possible to launch the attack remotely. The name of the patch is 974f21aa1b2527ef39c8afe1a5060548217deca8. It is recommended to apply a patch to fix this issue. VDB-216498 is the identifier assigned to this vulnerability.	4.3	More Details
CVE-2022-41654	An authentication bypass vulnerability exists in the newsletter subscription functionality of Ghost Foundation Ghost 5.9.4. A specially-crafted HTTP request can lead to increased privileges. An attacker can send an HTTP request to trigger this vulnerability.	4.3	More Details
CVE-2022-4741	A vulnerability was found in docconv up to 1.2.0 and classified as problematic. This issue affects the function ConvertDocx/ConvertODT/ConvertPages/ConvertXML/XMLToText. The manipulation leads to uncontrolled memory allocation. The attack may be initiated remotely. Upgrading to version 1.2.1 is able to address this issue. The name of the patch is 42bcff666855ab978e67a9041d0cdea552f20301. It is recommended to upgrade the affected component. The associated identifier of this vulnerability is VDB-216779.	4.3	More Details
CVE-2022-4633	A vulnerability was found in Auto Upload Images up to 3.3.0 and classified as problematic. Affected by this issue is some unknown functionality of the file src/setting-page.php of the component Settings Handler. The manipulation leads to cross-site request forgery. The attack may be launched remotely. Upgrading to version 3.3.1 is able to address this issue. The name of the patch is 895770ee93887ec78429c78ffdfb865bee6f9436. It is recommended to upgrade the affected component. VDB-216482 is the identifier assigned to this vulnerability.	4.3	More Details
CVE-2022-4738	A vulnerability classified as problematic has been found in SourceCodester Blood Bank Management System 1.0. Affected is an unknown function of the file index.php?page=users of the component User Registration Handler. The manipulation of the argument Name leads to cross site scripting. It is possible to launch the attack remotely. VDB-216774 is the identifier assigned to this vulnerability.	4.3	More Details
CVE-2021-4273	A vulnerability classified as problematic was found in studygolang. This vulnerability affects the function Search of the file http/controller/search.go. The manipulation of the argument q leads to cross site scripting. The attack can be initiated remotely. The exploit has been disclosed to the public and may be used. The name of the patch is 97ba556d42fa89dfaa7737e9cd3a8ddaf670bb23. It is recommended to apply a patch to fix this issue. VDB-216478 is the identifier assigned to this vulnerability.	4.3	More Details
CVE-2021-4280	A vulnerability was found in styler_praat_scripts. It has been classified as problematic. Affected is an unknown function of the file file_segmenter.praat of the component Slash Handler. The manipulation leads to denial of service. It is possible to launch the attack remotely. The name of the patch is 0cad44aa4a3eb0ecdba071c10eaff16023d8b35f. It is recommended to apply a patch to fix this issue. The identifier of this vulnerability is VDB-216780.	4.3	More Details
CVE-2021-4268	A vulnerability, which was classified as problematic, was found in phpRedisAdmin up to 1.17.3. This affects an unknown part. The manipulation leads to cross-site request forgery. It is possible to initiate the attack remotely. Upgrading to version 1.18.0 is able to address this issue. The name of the patch is b9039adbb264c81333328faa9575ecf8e0d2be94. It is recommended to upgrade the affected component. The associated identifier of this vulnerability is VDB-216471.	4.3	More Details
CVE-2020-36623	A vulnerability was found in Pengu. It has been declared as problematic. Affected by this vulnerability is the function runApp of the file src/index.js. The manipulation leads to cross-site request forgery. The attack can be launched remotely. The name of the patch is aea66f12b8cdfc3c8c50ad6a9c89d8307e9d0a91. It is recommended to apply a patch to fix this issue. The associated identifier of this vulnerability is VDB-216475.	4.3	More Details
CVE-2020-36622	A vulnerability was found in sah-comp bienlein and classified as problematic. This issue affects some unknown processing. The manipulation leads to cross-site request forgery. The attack may be initiated remotely. The name of the patch is d7836a4f2b241e4745ede194f0f6fb47199cab6b. It is recommended to apply a patch to fix this issue. The identifier VDB-216473 was assigned to this vulnerability.	4.3	More Details
CVE-2022-2582	The AWS S3 Crypto SDK sends an unencrypted hash of the plaintext alongside the ciphertext as a metadata field. This hash can be used to brute force the plaintext, if the hash is readable to the attacker. AWS now blocks this metadata field, but older SDK versions still send it.	4.3	More Details
CVE-2022-3034	When receiving an HTML email that specified to load an <code>iframe</code> element from a remote location, a request to the remote document was sent. However, Thunderbird didn't display the document. This vulnerability affects Thunderbird < 102.2.1 and Thunderbird < 91.13.1.	4.3	More Details
CVE-2022-43860	IBM Navigator for i 7.3, 7.4, and 7.5 could allow an authenticated user to obtain sensitive information they are authorized to but not while using this interface. By performing an SQL injection an attacker could see user profile attributes through this interface. IBM X-Force ID: 239305.	4.3	More Details

CVE Number	Description	Base Score	Reference
CVE-2022-34472	If there was a PAC URL set and the server that hosts the PAC was not reachable, OCSP requests would have been blocked, resulting in incorrect error pages being shown. This vulnerability affects Firefox < 102, Firefox ESR < 91.11, Thunderbird < 102, and Thunderbird < 91.11.	4.3	More Details
CVE-2021-4221	If a domain name contained a RTL character, it would cause the domain to be rendered to the right of the path. This could lead to user confusion and spoofing attacks. *This bug only affects Firefox for Android. Other operating systems are unaffected.* *Note*: Due to a clerical error this advisory was not included in the original announcement, and was added in Feburary 2022. This vulnerability affects Firefox < 92.	4.3	More Details
CVE-2022-26383	When resizing a popup after requesting fullscreen access, the popup would not display the fullscreen notification. This vulnerability affects Firefox < 98, Firefox ESR < 91.7, and Thunderbird < 91.7.	4.3	More Details
CVE-2022-29915	The Performance API did not properly hide the fact whether a request cross-origin resource has observed redirects. This vulnerability affects Firefox < 100.	4.3	More Details
CVE-2022-22749	When scanning QR codes, Firefox for Android would have allowed navigation to some URLs that do not point to web content. *This bug only affects Firefox for Android. Other operating systems are unaffected.*. This vulnerability affects Firefox < 96.	4.3	More Details
CVE-2022-31745	If array shift operations are not used, the Garbage Collector may have become confused about valid objects. This vulnerability affects Firefox < 101.	4.3	More Details
CVE-2022-22743	When navigating from inside an iframe while requesting fullscreen access, an attacker-controlled tab could have made the browser unable to leave fullscreen mode. This vulnerability affects Firefox ESR < 91.5, Firefox < 96, and Thunderbird < 91.5.	4.3	More Details
CVE-2022-22762	Under certain circumstances, a JavaScript alert (or prompt) could have been shown while another website was displayed underneath it. This could have been abused to trick the user. *This bug only affects Firefox for Android. Other operating systems are unaffected.*. This vulnerability affects Firefox < 97.	4.3	More Details
CVE-2022-1520	When viewing an email message A, which contains an attached message B, where B is encrypted or digitally signed or both, Thunderbird may show an incorrect encryption or signature status. After opening and viewing the attached message B, when returning to the display of message A, the message A might be shown with the security status of message B. This vulnerability affects Thunderbird < 91.9.	4.3	More Details
CVE-2022-26382	While the text displayed in Autofill tooltips cannot be directly read by JavaScript, the text was rendered using page fonts. Side-channel attacks on the text by using specially crafted fonts could have lead to this text being inferred by the webpage. This vulnerability affects Firefox < 98.	4.3	More Details
CVE-2022-36315	When loading a script with Subresource Integrity, attackers with an injection capability could trigger the reuse of previously cached entries with incorrect, different integrity metadata. This vulnerability affects Firefox < 103.	4.3	More Details
CVE-2022-22456	IBM Security Verify Governance, Identity Manager 10.0.1 is vulnerable to cross-site scripting. This vulnerability allows users to embed arbitrary JavaScript code in the Web UI thus altering the intended functionality potentially leading to credentials disclosure within a trusted session. IBM X-Force ID: 225004.	4.2	More Details
CVE-2021-4276	** UNSUPPORTED WHEN ASSIGNED ** A vulnerability was found in dns-stats hedgehog. It has been rated as problematic. Affected by this issue is the function DSCIOManager::dsc_import_input_from_source of the file src/DSCIOManager.cpp. The manipulation leads to sql injection. The attack may be launched remotely. The exploit has been disclosed to the public and may be used. The real existence of this vulnerability is still doubted at the moment. The name of the patch is 58922c345d3d1fe89bb2020111873a3e07ca93ac. It is recommended to apply a patch to fix this issue. VDB-216746 is the identifier assigned to this vulnerability. NOTE: This vulnerability only affects products that are no longer supported by the maintainer. NOTE: We do assume that the Data Manager server can only be accessed by authorised users. Because of this, we don't believe this specific attack is possible without such a compromise of the Data Manager server.	4.1	More Details
CVE-2022-2583	A race condition can cause incorrect HTTP request routing.	3.7	More Details

CVE Number	Description	Base Score	Reference
CVE-2019-25091	A vulnerability classified as problematic has been found in nsupdate.info. This affects an unknown part of the file src/nsupdate/settings/base.py of the component CSRF Cookie Handler. The manipulation of the argument CSRF_COOKIE_HTTPONLY leads to cookie without 'httponly' flag. It is possible to initiate the attack remotely. The name of the patch is 60a3fe559c453bc36b0ec3e5dd39c1303640a59a. It is recommended to apply a patch to fix this issue. The identifier VDB-216909 was assigned to this vulnerability.	3.7	More Details
CVE-2022-45430	Some Dahua software products have a vulnerability of unauthenticated enable or disable SSHD service. After bypassing the firewall access control policy, by sending a specific crafted packet to the vulnerable interface, an attacker could enable or disable the SSHD service.	3.7	More Details
CVE-2022-45433	Some Dahua software products have a vulnerability of unauthenticated traceroute host from remote DSS Server. After bypassing the firewall access control policy, by sending a specific crafted packet to the vulnerable interface, an attacker could get the traceroute results.	3.7	More Details
CVE-2022-4735	A vulnerability classified as problematic was found in asrashley dash-live. This vulnerability affects the function ready of the file static/js/media.js of the component DOM Node Handler. The manipulation leads to cross site scripting. The attack can be initiated remotely. The name of the patch is 24d01757a5319cc14c4aa1d8b53d1ab24d48e451. It is recommended to apply a patch to fix this issue. VDB-216766 is the identifier assigned to this vulnerability.	3.5	More Details
CVE-2021-4269	A vulnerability has been found in SimpleRisk and classified as problematic. This vulnerability affects the function checkAndSetValidation of the file simplerisk/js/common.js. The manipulation of the argument title leads to cross site scripting. The attack can be initiated remotely. Upgrading to version 20220306-001 is able to address this issue. The name of the patch is 591405b4ed160fbefc1dca1e55c5745079a7bb48. It is recommended to upgrade the affected component. The identifier of this vulnerability is VDB-216472.	3.5	More Details
CVE-2021-4272	A vulnerability classified as problematic has been found in studygolang. This affects an unknown part of the file static/js/topics.js. The manipulation of the argument contentHtml leads to cross site scripting. It is possible to initiate the attack remotely. The name of the patch is 0fb30f9640bd5fa0cae58922eac6c00bb1a94391. It is recommended to apply a patch to fix this issue. The identifier VDB-216477 was assigned to this vulnerability.	3.5	More Details
CVE-2021-4271	A vulnerability was found in panicsteve w2wiki. It has been rated as problematic. Affected by this issue is the function toHTML of the file index.php of the component Markdown Handler. The manipulation leads to cross site scripting. The attack may be launched remotely. The name of the patch is 8f1d0470b4ddb1c7699e3308e765c11ed29542b6. It is recommended to apply a patch to fix this issue. The identifier of this vulnerability is VDB-216476.	3.5	More Details
CVE-2021-4292	A vulnerability was found in OpenMRS Admin UI Module up to 1.4.x. It has been rated as problematic. This issue affects some unknown processing of the file omod/src/main/webapp/pages/metadata/privileges/privilege.gsp of the component Manage Privilege Page. The manipulation leads to cross site scripting. The attack may be initiated remotely. Upgrading to version 1.5.0 is able to address this issue. The name of the patch is 4f8565425b7c74128dec9ca46dfbb9a3c1c24911. It is recommended to upgrade the affected component. The identifier VDB-216917 was assigned to this vulnerability.	3.5	More Details
CVE-2021-4291	A vulnerability was found in OpenMRS Admin UI Module up to 1.5.x. It has been declared as problematic. This vulnerability affects unknown code of the file omod/src/main/webapp/pages/metadata/locations/location.gsp. The manipulation leads to cross site scripting. The attack can be initiated remotely. Upgrading to version 1.6.0 is able to address this issue. The name of the patch is a7eefb5f69f6c50a3bffcb138bb8ea57cb41a9b6. It is recommended to upgrade the affected component. The identifier of this vulnerability is VDB-216916.	3.5	More Details
CVE-2021-4270	A vulnerability was found in Imprint CMS. It has been classified as problematic. Affected is the function SearchForm of the file ImprintCMS/Models/ViewHelpers.cs. The manipulation of the argument query leads to cross site scripting. It is possible to launch the attack remotely. The name of the patch is 6140b140ccd02b5e4e7d6ba013ac1225724487f4. It is recommended to apply a patch to fix this issue. VDB-216474 is the identifier assigned to this vulnerability.	3.5	More Details
CVE-2022-4736	A vulnerability was found in Venganzas del Pasado and classified as problematic. Affected by this issue is some unknown functionality. The manipulation of the argument the_title leads to cross site scripting. The attack may be launched remotely. The name of the patch is 62339b2ec445692c710b804bdf07aef4bd247ff7. It is recommended to apply a patch to fix this issue. VDB-216770 is the identifier assigned to this vulnerability.	3.5	More Details

CVE Number	Description	Base Score	Reference
CVE-2020-36636	A vulnerability classified as problematic has been found in OpenMRS Admin UI Module up to 1.4.x. Affected is the function sendErrorMessage of the file omod/src/main/java/org/openmrs/module/adminui/page/controller/systemadmin/accounts/AccountPageController.java of the component Account Setup Handler. The manipulation leads to cross site scripting. It is possible to launch the attack remotely. Upgrading to version 1.5.0 is able to address this issue. The name of the patch is 702fbfdac7c4418f23bb5f6452482b4a88020061. It is recommended to upgrade the affected component. VDB-216918 is the identifier assigned to this vulnerability.	3.5	More Details
CVE-2019-25084	A vulnerability, which was classified as problematic, has been found in Hide Files on GitHub up to 2.x. This issue affects the function addEventListener of the file extension/options.js. The manipulation leads to cross site scripting. The attack may be initiated remotely. Upgrading to version 3.0.0 is able to address this issue. The name of the patch is 9de0c57df81db1178e0e79431d462f6d9842742e. It is recommended to upgrade the affected component. The associated identifier of this vulnerability is VDB-216767.	3.5	More Details
CVE-2020-36635	A vulnerability was found in OpenMRS Appointment Scheduling Module up to 1.12.x. It has been classified as problematic. This affects the function validateFieldName of the file api/src/main/java/org/openmrs/module/appointmentscheduling/validator/AppointmentTypeValidator.java. The manipulation leads to cross site scripting. It is possible to initiate the attack remotely. Upgrading to version 1.13.0 is able to address this issue. The name of the patch is 34213c3f6ea22df427573076fb62744694f601d8. It is recommended to upgrade the affected component. The associated identifier of this vulnerability is VDB-216915.	3.5	More Details
CVE-2021-4267	A vulnerability classified as problematic was found in tad_discuss. Affected by this vulnerability is an unknown functionality. The manipulation of the argument DiscussTitle leads to cross site scripting. The attack can be launched remotely. The name of the patch is af94d034ff8db642d05fd8788179eab05f433958. It is recommended to apply a patch to fix this issue. The identifier VDB-216469 was assigned to this vulnerability.	3.5	More Details
CVE-2021-4266	A vulnerability classified as problematic has been found in Webdetails cpf up to 9.5.0.0-80. Affected is an unknown function of the file core/src/main/java/pt/webdetails/cpf/packager/DependenciesPackage.java. The manipulation of the argument baseUrl leads to cross site scripting. It is possible to launch the attack remotely. Upgrading to version 9.5.0.0-81 is able to address this issue. The name of the patch is 3bff900d228e8cae3af256b447c5d15bdb03c174. It is recommended to upgrade the affected component. The identifier of this vulnerability is VDB-216468.	3.5	More Details
CVE-2021-4265	A vulnerability was found in siwapp-ror. It has been rated as problematic. This issue affects some unknown processing. The manipulation leads to cross site scripting. The attack may be initiated remotely. The name of the patch is 924d16008cfcc09356c87db01848e45290cb58ca. It is recommended to apply a patch to fix this issue. The associated identifier of this vulnerability is VDB-216467.	3.5	More Details
CVE-2021-4263	A vulnerability, which was classified as problematic, has been found in leanote 2.6.1. This issue affects the function define of the file public/js/plugins/history.js. The manipulation of the argument content leads to cross site scripting. The attack may be initiated remotely. The identifier of the patch is 0f9733c890077942150696dcc6d2b1482b7a0a19. It is recommended to apply a patch to fix this issue. The identifier VDB-216461 was assigned to this vulnerability.	3.5	More Details
CVE-2020-36621	A vulnerability, which was classified as problematic, has been found in chedabob whatismyudid. Affected by this issue is the function exports.enrollment of the file routes/mobileconfig.js. The manipulation leads to cross site scripting. The attack may be launched remotely. The name of the patch is bb33d4325fba80e7ea68b79121dba025caf6f45f. It is recommended to apply a patch to fix this issue. VDB-216470 is the identifier assigned to this vulnerability.	3.5	More Details
CVE-2020-36620	A vulnerability was found in Brondahl EnumStringValues up to 4.0.0. It has been declared as problematic. This vulnerability affects the function GetStringValuesWithPreferences_Uncache of the file EnumStringValues/EnumExtensions.cs. The manipulation leads to resource consumption. Upgrading to version 4.0.1 is able to address this issue. The name of the patch is c0fc7806beb24883cc2f9543ebc50c0820297307. It is recommended to upgrade the affected component. VDB-216466 is the identifier assigned to this vulnerability.	3.5	More Details
CVE-2019-25088	A vulnerability was found in ytti Oxidized Web. It has been classified as problematic. Affected is an unknown function of the file lib/oxidized/web/views/conf_search.haml. The manipulation of the argument to_research leads to cross site scripting. It is possible to launch the attack remotely. The name of the patch is 55ab9bdc68b03ebce9280b8746ef31d7fdedcc45. It is recommended to apply a patch to fix this issue. VDB-216870 is the identifier assigned to this vulnerability.	3.5	More Details

CVE Number	Description	Base Score	Reference
CVE-2021-4274	A vulnerability, which was classified as problematic, has been found in sileht bird-lg. This issue affects some unknown processing of the file templates/layout.html. The manipulation of the argument request_args leads to cross site scripting. The attack may be initiated remotely. The name of the patch is ef6b32c527478fefe7a4436e10b96ee28ed5b308. It is recommended to apply a patch to fix this issue. The associated identifier of this vulnerability is VDB-216479.	3.5	More Details
CVE-2021-4282	A vulnerability was found in FreePBX voicemail. It has been declared as problematic. Affected by this vulnerability is an unknown functionality of the file page.voicemail.php. The manipulation leads to cross site scripting. The attack can be launched remotely. Upgrading to version 14.0.6.25 is able to address this issue. The name of the patch is 12e1469ef9208eda9d8955206e78345949236ee6. It is recommended to upgrade the affected component. The associated identifier of this vulnerability is VDB-216871.	3.5	More Details
CVE-2022-4638	A vulnerability classified as problematic was found in collective.contact.widget up to 1.12. This vulnerability affects the function title of the file src/collective/contact/widget/widgets.py. The manipulation leads to cross site scripting. The attack can be initiated remotely. The name of the patch is 5da36305ca7ed433782be8901c47387406fcda12. It is recommended to apply a patch to fix this issue. The identifier of this vulnerability is VDB-216496.	3.5	More Details
CVE-2021-4284	A vulnerability classified as problematic has been found in OpenMRS HTML Form Entry UI Framework Integration Module up to 1.x. This affects an unknown part. The manipulation leads to cross site scripting. It is possible to initiate the attack remotely. Upgrading to version 2.0.0 is able to address this issue. The name of the patch is 811990972ea07649ae33c4b56c61c3b520895f07. It is recommended to upgrade the affected component. The identifier VDB-216873 was assigned to this vulnerability.	3.5	More Details
CVE-2022-4755	A vulnerability was found in FlatPress and classified as problematic. This issue affects the function main of the file fp-plugins/mediamanager/panels/panel.mediamanager.file.php of the component Media Manager Plugin. The manipulation of the argument mm-newgallery-name leads to cross site scripting. The attack may be initiated remotely. The name of the patch is d3f329496536dc99f9707f2f295d571d65a496f5. It is recommended to apply a patch to fix this issue. The identifier VDB-216869 was assigned to this vulnerability.	3.5	More Details
CVE-2021-4285	A vulnerability classified as problematic was found in Nagios NCPA. This vulnerability affects unknown code of the file agent/listener/templates/tail.html. The manipulation of the argument name leads to cross site scripting. The attack can be initiated remotely. Upgrading to version 2.4.0 is able to address this issue. The name of the patch is 5abbcd7aa26e0fc815e6b2b0ffe1c15ef3e8fab5. It is recommended to upgrade the affected component. VDB-216874 is the identifier assigned to this vulnerability.	3.5	More Details
CVE-2019-25090	A vulnerability was found in FreePBX arimanager up to 13.0.5.3 and classified as problematic. Affected by this issue is some unknown functionality of the component Views Handler. The manipulation of the argument dataurl leads to cross site scripting. The attack may be launched remotely. Upgrading to version 13.0.5.4 is able to address this issue. The name of the patch is 199dea7cc7020d3c469a86a39fbd80f5edd3c5ab. It is recommended to upgrade the affected component. VDB-216878 is the identifier assigned to this vulnerability.	3.5	More Details
CVE-2019-25086	A vulnerability was found in IET-OU Open Media Player up to 1.5.0. It has been declared as problematic. This vulnerability affects the function webvtt of the file application/controllers/timedtext.php. The manipulation of the argument ttml_url leads to cross site scripting. The attack can be initiated remotely. Upgrading to version 1.5.1 is able to address this issue. The name of the patch is 3f39f2d68d11895929c04f7b49b97a734ae7cd1f. It is recommended to upgrade the affected component. VDB-216862 is the identifier assigned to this vulnerability.	3.5	More Details
CVE-2021-4288	A vulnerability was found in OpenMRS openmrs-module-referenceapplication up to 2.11.x. It has been rated as problematic. This issue affects some unknown processing of the file omod/src/main/webapp/pages/userApp.gsp. The manipulation leads to cross site scripting. The attack may be initiated remotely. Upgrading to version 2.12.0 is able to address this issue. The name of the patch is 35f81901a4cb925747a9615b8706f5079d2196a1. It is recommended to upgrade the affected component. The identifier VDB-216881 was assigned to this vulnerability.	3.5	More Details
CVE-2022-4631	A vulnerability, which was classified as problematic, was found in WP-Ban. Affected is an unknown function of the file ban-options.php. The manipulation leads to cross site scripting. It is possible to launch the attack remotely. The name of the patch is 22b925449c84faa9b7496abe4f8f5661cb5eb3bf. It is recommended to upgrade the affected component. The identifier of this vulnerability is VDB-216480.	3.5	More Details
CVE-2015-10005	A vulnerability was found in markdown-it up to 2.x. It has been classified as problematic. Affected is an unknown function of the file lib/common/html_re.js. The manipulation leads to inefficient regular expression complexity. Upgrading to version 3.0.0 is able to address this issue. The name of the patch is 89c8620157d6e38f9872811620d25138fc9d1b0d. It is recommended to upgrade the affected component. The identifier of this vulnerability is VDB-216852.	3.5	More Details

CVE Number	Description	Base Score	Reference
CVE-2022-4640	A vulnerability has been found in Mingsoft MCMS 5.2.9 and classified as problematic. Affected by this vulnerability is the function save of the component Article Handler. The manipulation leads to cross site scripting. The attack can be launched remotely. The exploit has been disclosed to the public and may be used. It is recommended to upgrade the affected component. The associated identifier of this vulnerability is VDB-216499.	3.5	More Details
CVE-2021-4289	A vulnerability classified as problematic was found in OpenMRS openmrs-module-referenceapplication up to 2.11.x. Affected by this vulnerability is the function post of the file omod/src/main/java/org/openmrs/module/referenceapplication/page/controller/UserAppPageController.java of the component User App Page. The manipulation of the argument AppId leads to cross site scripting. The attack can be launched remotely. Upgrading to version 2.12.0 is able to address this issue. The name of the patch is 0410c091d46eed3c132fe0fcafe5964182659f74. It is recommended to upgrade the affected component. The associated identifier of this vulnerability is VDB-216883.	3.5	More Details
CVE-2022-4730	A vulnerability was found in Graphite Web. It has been classified as problematic. Affected is an unknown function of the component Absolute Time Range Handler. The manipulation leads to cross site scripting. It is possible to launch the attack remotely. The exploit has been disclosed to the public and may be used. The name of the patch is 2f178f490e10efc03cd1d27c72f64ecab224eb23. It is recommended to apply a patch to fix this issue. The identifier of this vulnerability is VDB-216744.	3.5	More Details
CVE-2022-4740	A vulnerability, which was classified as problematic, has been found in kkFileView. Affected by this issue is the function setWatermarkAttribute of the file /picturesPreview. The manipulation 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-216776.	3.5	More Details
CVE-2022-4642	A vulnerability was found in tatoeba2. It has been classified as problematic. This affects an unknown part of the component Profile Name Handler. The manipulation 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. Upgrading to version prod_2022-10-30 is able to address this issue. The name of the patch is 91110777fc8ddf1b4a2cf4e66e67db69b9700361. It is recommended to upgrade the affected component. The identifier VDB-216501 was assigned to this vulnerability.	3.5	More Details
CVE-2022-4727	A vulnerability, which was classified as problematic, was found in OpenMRS Appointment Scheduling Module up to 1.16.x. This affects the function getNotes of the file api/src/main/java/org/openmrs/module/appointmentscheduling/AppointmentRequest.java of the component Notes Handler. The manipulation of the argument notes leads to cross site scripting. It is possible to initiate the attack remotely. Upgrading to version 1.17.0 is able to address this issue. The name of the patch is 2ccbe39c020809765de41eeb8ee4c70b5ec49cc8. It is recommended to upgrade the affected component. The identifier VDB-216741 was assigned to this vulnerability.	3.5	More Details
CVE-2022-4728	A vulnerability has been found in Graphite Web and classified as problematic. This vulnerability affects unknown code of the component Cookie Handler. The manipulation leads to cross site scripting. The attack can be initiated remotely. The exploit has been disclosed to the public and may be used. The name of the patch is 2f178f490e10efc03cd1d27c72f64ecab224eb23. It is recommended to apply a patch to fix this issue. VDB-216742 is the identifier assigned to this vulnerability.	3.5	More Details
CVE-2022-4729	A vulnerability was found in Graphite Web and classified as problematic. This issue affects some unknown processing of the component Template Name Handler. The manipulation leads to cross site scripting. The attack may be initiated remotely. The exploit has been disclosed to the public and may be used. The name of the patch is 2f178f490e10efc03cd1d27c72f64ecab224eb23. It is recommended to apply a patch to fix this issue. The associated identifier of this vulnerability is VDB-216743.	3.5	More Details
CVE-2022-4637	A vulnerability classified as problematic has been found in ep3-bs up to 1.7.x. This affects an unknown part. The manipulation leads to cross site scripting. It is possible to initiate the attack remotely. Upgrading to version 1.8.0 is able to address this issue. The name of the patch is ef49e709c8adecc3a83cdc6164a67162991d2213. It is recommended to upgrade the affected component. The associated identifier of this vulnerability is VDB-216495.	3.5	More Details
CVE-2022-4632	A vulnerability has been found in Auto Upload Images up to 3.3.0 and classified as problematic. Affected by this vulnerability is an unknown functionality. The manipulation leads to cross site scripting. The attack can be launched remotely. Upgrading to version 3.3.1 is able to address this issue. The name of the patch is 895770ee93887ec78429c78ffdfb865bee6f9436. It is recommended to upgrade the affected component. The identifier VDB-216481 was assigned to this vulnerability.	3.5	More Details
CVE-2022-42931	Logins saved by Firefox should be managed by the Password Manager component which uses encryption to save files on-disk. Instead, the username (not password) was saved by the Form Manager to an unencrypted file on disk. This vulnerability affects Firefox < 106.	3.3	More Details

CVE Number	Description	Base Score	Reference
CVE-2022-41977	An out of bounds read vulnerability exists in the way OpenImageIO version v2.3.19.0 processes string fields in TIFF image files. A specially-crafted TIFF file can lead to information disclosure. An attacker can provide a malicious file to trigger this vulnerability.	3.3	More Details
CVE-2019-25089	A vulnerability has been found in Morgawr Muon 0.1.1 and classified as problematic. Affected by this vulnerability is an unknown functionality of the file src/muon/handler.clj. The manipulation leads to insufficiently random values. The attack can be launched remotely. Upgrading to version 0.2.0-indev is able to address this issue. The name of the patch is c09ed972c020f759110c707b06ca2644f0bacd7f. It is recommended to upgrade the affected component. The identifier VDB-216877 was assigned to this vulnerability.	3.1	More Details
CVE-2018-25049	A vulnerability was found in email-existence. It has been rated as problematic. Affected by this issue is some unknown functionality of the file index.js. The manipulation leads to inefficient regular expression complexity. The name of the patch is 0029ba71b6ad0d8ec0baa2ecc6256d038bdd9b56. It is recommended to apply a patch to fix this issue. VDB-216854 is the identifier assigned to this vulnerability.	3.0	More Details
CVE-2022-45428	Some Dahua software products have a vulnerability of sensitive information leakage. After obtaining the permissions of administrators, by sending a specific crafted packet to the vulnerable interface, an attacker can obtain the debugging information.	2.7	More Details
CVE-2020-36634	A vulnerability classified as problematic has been found in Indeed Engineering util up to 1.0.33. Affected is the function visit/appendTo of the file varexport/src/main/java/com/indeed/util/varexport/servlet/ViewExportedVariablesServlet.java. The manipulation leads to cross site scripting. It is possible to launch the attack remotely. Upgrading to version 1.0.34 is able to address this issue. The name of the patch is c0952a9db51a880e9544d9fac2a2218a6bfc9c63. It is recommended to upgrade the affected component. VDB-216882 is the identifier assigned to this vulnerability.	2.6	More Details
CVE-2021-4277	A vulnerability, which was classified as problematic, has been found in fredsmith utils. This issue affects some unknown processing of the file screenshot_sync of the component Filename Handler. The manipulation leads to predictable from observable state. The name of the patch is dbab1b66955eeb3d76b34612b358307f5c4e3944. It is recommended to apply a patch to fix this issue. The identifier VDB-216749 was assigned to this vulnerability.	2.6	More Details
CVE-2021-4286	A vulnerability, which was classified as problematic, has been found in cocagne pysrp up to 1.0.16. This issue affects the function calculate_x of the file srp/_ctsrp.py. The manipulation leads to information exposure through discrepancy. Upgrading to version 1.0.17 is able to address this issue. The name of the patch is dba52642f5e95d3da7af1780561213ee6053195f. It is recommended to upgrade the affected component. The associated identifier of this vulnerability is VDB-216875.	2.6	More Details
CVE-2022-4641	A vulnerability was found in pig-vector and classified as problematic. Affected by this issue is the function LogisticRegression of the file src/main/java/org/apache/mahout/pig/LogisticRegression.java. The manipulation leads to insecure temporary file. The attack needs to be approached locally. The name of the patch is 1e7bd9fab5401a2df18d2eabd802adcf0dcf1f15. It is recommended to apply a patch to fix this issue. The identifier of this vulnerability is VDB-216500.	2.5	More Details
CVE-2022-4731	A vulnerability, which was classified as problematic, was found in myapnea up to 29.0.x. Affected is an unknown function of the component Title Handler. The manipulation leads to cross site scripting. It is possible to launch the attack remotely. Upgrading to version 29.1.0 is able to address this issue. The name of the patch is 99934258530d761bd5d09809bfa6c14b598f8d18. It is recommended to upgrade the affected component. VDB-216750 is the identifier assigned to this vulnerability.	2.4	More Details
CVE-2021-4283	A vulnerability was found in FreeBPX voicemail. It has been rated as problematic. Affected by this issue is some unknown functionality of the file views/ssettings.php of the component Settings Handler. The manipulation of the argument key leads to cross site scripting. The attack may be launched remotely. Upgrading to version 14.0.6.25 is able to address this issue. The name of the patch is ffce4882016076acd16fe0f676246905aa3cb2f3. It is recommended to upgrade the affected component. The identifier of this vulnerability is VDB-216872.	2.4	More Details
CVE-2022-4516	Rejected reason: DO NOT USE THIS CANDIDATE NUMBER. ConsultIDs: none. Reason: This candidate was in a CNA pool that was not assigned to any issues during 2022. Notes: none.	N/A	More Details
CVE-2022-4685	Rejected reason: DO NOT USE THIS CANDIDATE NUMBER. Reason: This CVE has been rejected as it was incorrectly assigned. All references and descriptions in this candidate have been removed to prevent accidental usage.	N/A	More Details

CVE Number	Description	Base Score	Reference
CVE-2022-23529	Rejected reason: DO NOT USE THIS CANDIDATE NUMBER. ConsultIDs: none. Reason: The issue is not a vulnerability. Notes: none.	N/A	More Details