SingCERT
Singapore Cyber Emergency Response Team

# Security Bulletin 30 June 2021

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-2021-29485 | Ratpack is a toolkit for creating web applications. In versions prior to 1.9.0, a malicious attacker can achieve Remote Code Execution (RCE) via a maliciously crafted Java deserialization gadget chain leveraged against the Ratpack session store. If one's application does not use Ratpack's session mechanism, it is not vulnerable. Ratpack 1.9.0 introduces a strict allow-list mechanism that mitigates this vulnerability when used. Two possible workarounds exist. The simplest mitigation for users of earlier versions is to reduce the likelihood of attackers being able to write to the session data store. Alternatively or additionally, the allow-list mechanism could be manually back ported by providing an alternative implementation of `SessionSerializer` that uses an allow-list. | 9.9 | More Details |
| CVE-2021-35049 | Vulnerability in Fidelis Network and Deception CommandPost enables authenticated command injection through the web interface. The vulnerability could allow a specially crafted HTTP request to execute system commands on the CommandPost and return results in an HTTP response in an authenticated session. The vulnerability is present in Fidelis Network and Deception versions prior to 9.3.7 and in version 9.4. Patches and updates are available to address this vulnerability. | 9.9 | More Details |
| CVE-2021-35047 | Vulnerability in the CommandPost, Collector, and Sensor components of Fidelis Network and Deception enables an attacker with user level access to the CLI to inject root level commands into the component and neighboring Fidelis components. The vulnerability is present in Fidelis Network and Deception versions prior to 9.3.7 and in version 9.4. Patches and updates are available to address this vulnerability. | 9.9 | More Details |
| CVE-2021-32990 | FATEK Automation WinProladder Versions 3.30 and prior are vulnerable to an out-of-bounds read, which may allow an attacker to execute arbitrary code. | 9.8 | More Details |
| CVE-2021-32988 | FATEK Automation WinProladder Versions 3.30 and prior are vulnerable to an out-of-bounds write, which may allow an attacker to execute arbitrary code. | 9.8 | More Details |
| CVE-2021-31531 | Zoho ManageEngine ServiceDesk Plus MSP before 10521 is vulnerable to Server-Side Request Forgery (SSRF). | 9.8 | More Details |
| CVE-2020-23711 | SQL Injection vulnerability in NavigateCMS 2.9 via the URL encoded GET input category in navigate.php. | 9.8 | More Details |
| CVE-2021-34187 | main/inc/ajax/model.ajax.php in Chamilo through 1.11.14 allows SQL Injection via the searchField, filters, or filters2 parameter. | 9.8 | More Details |
| CVE-2021-21998 | VMware Carbon Black App Control 8.0, 8.1, 8.5 prior to 8.5.8, and 8.6 prior to 8.6.2 has an authentication bypass. A malicious actor with network access to the VMware Carbon Black App Control management server might be able to obtain administrative access to the product without the need to authenticate. | 9.8 | More Details |
| CVE-2021-31337 | The Telnet service of the SIMATIC HMI Comfort Panels system component in affected products does not require authentication, which may allow a remote attacker to gain access to the device if the service is enabled. Telnet is disabled by default on the SINAMICS Medium Voltage Products (SINAMICS SL150: All versions, SINAMICS SM150: All versions, SINAMICS SM150i: All versions). | 9.8 | More Details |
| CVE-2021-35514 | Narou (aka Narou.rb) before 3.8.0 allows Ruby Code Injection via the title name or author name of a novel. | 9.8 | More Details |
| CVE-2021-35502 | app/View/Elements/genericElements/IndexTable/Fields/generic_field.ctp in MISP 2.4.144 does not sanitize certain data related to generic-template:index. | 9.8 | More Details |

| CVE Number | Description | Base Score | Reference |
|---|---|---|---|
| CVE-2021-34427 | In Eclipse BIRT versions 4.8.0 and earlier, an attacker can use query parameters to create a JSP file which is accessible from remote (current BIRT viewer dir) to inject JSP code into the running instance. | 9.8 | More Details |
| CVE-2021-34074 | PandoraFMS <=7.54 allows arbitrary file upload, it leading to remote command execution via the File Manager. To bypass the built-in protection, a relative path is used in the requests. | 9.8 | More Details |
| CVE-2021-34184 | Miniaudio 0.10.35 has a Double free vulnerability that could cause a buffer overflow in ma_default_vfs_close__stdio in miniaudio.h. | 9.8 | More Details |
| CVE-2021-32992 | FATEK Automation WinProladder Versions 3.30 and prior do not properly restrict operations within the bounds of a memory buffer, which may allow an attacker to execute arbitrary code. | 9.8 | More Details |
| CVE-2021-35456 | Online Pet Shop We App 1.0 is vulnerable to remote SQL injection and shell upload | 9.8 | More Details |
| CVE-2021-27649 | Use after free vulnerability in file transfer protocol component in Synology DiskStation Manager (DSM) before 6.2.3-25426-3 allows remote attackers to execute arbitrary code via unspecified vectors. | 9.8 | More Details |
| CVE-2021-28958 | Zoho ManageEngine ADSelfService Plus through 6101 is vulnerable to unauthenticated Remote Code Execution while changing the password. | 9.8 | More Details |
| CVE-2020-21786 | In IBOS 4.5.4 Open, Arbitrary File Inclusion causes getshell via /system/modules/dashboard/controllers/CronController.php. | 9.8 | More Details |
| CVE-2020-20392 | SQL Injection vulnerability in imcat v5.2 via the fm[auser] parameters in coms/add_coms.php. | 9.8 | More Details |
| CVE-2021-29954 | Proxy functionality built into Hubs Cloud's Reticulum software allowed access to internal URLs, including the metadata service. This vulnerability affects Hubs Cloud < mozillareality/reticulum/1.0.1/20210428201255. | 9.8 | More Details |
| CVE-2020-21787 | CRMEB 3.1.0+ is vulnerable to File Upload Getshell via /crmeb/crmeb/services/UploadService.php. | 9.8 | More Details |
| CVE-2020-18662 | SQL Injection vulnerability in gnuboard5 <=v5.3.2.8 via the table_prefix parameter in install_db.php. | 9.8 | More Details |
| CVE-2020-21784 | phpwcms 1.9.13 is vulnerable to Code Injection via /phpwcms/setup/setup.php. | 9.8 | More Details |
| CVE-2021-31649 | In applications using jfinal 4.9.08 and below, there is a deserialization vulnerability when using redis,may be vulnerable to remote code execute | 9.8 | More Details |
| CVE-2021-33346 | There is an arbitrary password modification vulnerability in a D-LINK DSL-2888A router product. An attacker can use this vulnerability to modify the password of the admin user without authorization. | 9.8 | More Details |
| CVE-2020-18667 | SQL Injection vulnerability in WebPort <=1.19.1 via the new connection, parameter name in type-conn. | 9.8 | More Details |
| CVE-2021-32708 | Flysystem is an open source file storage library for PHP. The whitespace normalisation using in 1.x and 2.x removes any unicode whitespace. Under certain specific conditions this could potentially allow a malicious user to execute code remotely. The conditions are: A user is allowed to supply the path or filename of an uploaded file, the supplied path or filename is not checked against unicode chars, the supplied pathname checked against an extension deny-list, not an allow-list, the supplied path or filename contains a unicode whitespace char in the extension, the uploaded file is stored in a directory that allows PHP code to be executed. Given these conditions are met a user can upload and execute arbitrary code on the system under attack. The unicode whitespace removal has been replaced with a rejection (exception). For 1.x users, upgrade to 1.1.4. For 2.x users, upgrade to 2.1.1. | 9.8 | More Details |
| CVE-2020-17752 | Integer overflow vulnerability in payable function of a smart contract implementation for an Ethereum token, as demonstrated by the smart contract implemented at address 0xB49E984A83d7A638E7F2889fc8328952BA951AbE, an implementation for MillionCoin (MON). | 9.8 | More Details |
| CVE-2021-35048 | Vulnerability in Fidelis Network and Deception CommandPost enables unauthenticated SQL injection through the web interface. The vulnerability could lead to exposure of authentication tokens in some versions of Fidelis software. The vulnerability is present in Fidelis Network and Deception versions prior to 9.3.7 and in version 9.4. Patches and updates are available to address this vulnerability. | 9.8 | More Details |
| CVE-2020-7868 | A remote code execution vulnerability exists in helpUS(remote administration tool) due to improper validation of parameter of ShellExecutionExA function used for login. | 9.6 | More Details |

| CVE Number | Description | Base Score | Reference |
|---|---|---|---|
| CVE-2021-32711 | Shopware is an open source eCommerce platform. Versions prior to 6.3.5.1 may leak of information via Store-API. The vulnerability could only be fixed by changing the API system, which involves a non-backward-compatible change. Only consumers of the Store-API should be affected by this change. We recommend to update to the current version 6.3.5.1. You can get the update to 6.3.5.1 regularly via the Auto-Updater or directly via the download overview. https://www.shopware.com/en/download/#shopware-6 The vulnerability could only be fixed by changing the API system, which involves a non-backward-compatible change. Only consumers of the Store-API should be affected by this change. Please check your plugins if you have it in use. Detailed technical information can be found in the upgrade information. https://github.com/shopware/platform/blob/v6.3.5.1/UPGRADE-6.3.md#6351 ### Workarounds For older versions of 6.1 and 6.2, corresponding security measures are also available via a plugin. For the full range of functions, we recommend updating to the latest Shopware version. https://store.shopware.com/en/detail/index/sArticle/518463/number/Swag136939272659 ### For more information https://docs.shopware.com/en/shopware-6-en/security-updates/security-update-02-2021 | 9.1 | More Details |
| CVE-2021-21809 | A command execution vulnerability exists in the default legacy spellchecker plugin in Moodle 3.10. A specially crafted series of HTTP requests can lead to command execution. An attacker must have administrator privileges to exploit this vulnerabilities. | 9.1 | More Details |
| CVE-2020-7869 | An improper input validation vulnerability of ZOOK software (remote administration tool) could allow a remote attacker to create arbitrary file. The ZOOK viewer has the "Tight file CMD" function to create file. An attacker could create and execute arbitrary file in the ZOOK agent program using "Tight file CMD" without authority. | 9.0 | More Details |

## OTHER VULNERABILITIES

| CVE Number | Description | Base Score | Reference |
|---|---|---|---|
| CVE-2021-23994 | A WebGL framebuffer was not initialized early enough, resulting in memory corruption and an out of bound write. This vulnerability affects Firefox ESR < 78.10, Thunderbird < 78.10, and Firefox < 88. | 8.8 | More Details |
| CVE-2021-21102 | Adobe Illustrator version 25.2 (and earlier) is affected by a Path Traversal vulnerability when parsing a specially crafted file. An unauthenticated attacker could leverage this vulnerability to achieve arbitrary code execution in the context of the current user. Exploitation of this issue requires user interaction in that a victim must open a malicious file. | 8.8 | More Details |
| CVE-2021-29946 | Ports that were written as an integer overflow above the bounds of a 16-bit integer could have bypassed port blocking restrictions when used in the Alt-Svc header. This vulnerability affects Firefox ESR < 78.10, Thunderbird < 78.10, and Firefox < 88. | 8.8 | More Details |
| CVE-2021-33528 | In Weidmueller Industrial WLAN devices in multiple versions an exploitable privilege escalation vulnerability exists in the iw_console functionality. A specially crafted menu selection string can cause an escape from the restricted console, resulting in system access as the root user. An attacker can send commands while authenticated as a low privilege user to trigger this vulnerability. | 8.8 | More Details |
| CVE-2021-33530 | In Weidmueller Industrial WLAN devices in multiple versions an exploitable command injection vulnerability exists in encrypted diagnostic script functionality of the devices. A specially crafted diagnostic script file can cause arbitrary busybox commands to be executed, resulting in remote control over the device. An attacker can send diagnostic while authenticated as a low privilege user to trigger this vulnerability. | 8.8 | More Details |
| CVE-2021-33531 | In Weidmueller Industrial WLAN devices in multiple versions an exploitable use of hard-coded credentials vulnerability exists in multiple iw_* utilities. The device operating system contains an undocumented encryption password, allowing for the creation of custom diagnostic scripts. An attacker can send diagnostic scripts while authenticated as a low privilege user to trigger this vulnerability. | 8.8 | More Details |
| CVE-2021-33532 | In Weidmueller Industrial WLAN devices in multiple versions an exploitable command injection vulnerability exists in the iw_webs functionality. A specially crafted diagnostic script file name can cause user input to be reflected in a subsequent iw_system call, resulting in remote control over the device. An attacker can send commands while authenticated as a low privilege user to trigger this vulnerability. | 8.8 | More Details |
| CVE-2021-20574 | IBM Security Identity Manager Adapters 6.0 and 7.0 could allow a remote authenticated attacker to conduct an LDAP injection. By using a specially crafted request, an attacker could exploit this vulnerability and takeover other accounts. IBM X-Force ID: 199252. | 8.8 | More Details |
| CVE-2021-28588 | Adobe RoboHelp Server version 2019.0.9 (and earlier) is affected by a Path Traversal vulnerability when parsing a crafted HTTP POST request. An authenticated attacker could leverage this vulnerability to achieve arbitrary code execution in the context of the current user. Exploitation of this issue does not require user interaction. | 8.8 | More Details |
| CVE-2021-33533 | In Weidmueller Industrial WLAN devices in multiple versions an exploitable command injection vulnerability exists in the iw_webs functionality. A specially crafted iw_serverip parameter can cause user input to be reflected in a subsequent iw_system call, resulting in remote control over the device. An attacker can send commands while authenticated as a low privilege user to trigger this vulnerability. | 8.8 | More Details |
| CVE-2021-33535 | In Weidmueller Industrial WLAN devices in multiple versions an exploitable format string vulnerability exists in the iw_console conio_writestr functionality. A specially crafted time server entry can cause an overflow of the time server buffer, resulting in remote code execution. An attacker can send commands while authenticated as a low privilege user to trigger this vulnerability. | 8.8 | More Details |
| CVE-2021-28562 | Acrobat Reader DC versions versions 2021.001.20150 (and earlier), 2020.001.30020 (and earlier) and 2017.011.30194 (and earlier) are affected by a Use After Free vulnerability when executing search queries through Javascript. An unauthenticated attacker could leverage this vulnerability to achieve arbitrary code execution in the context of the current user. Exploitation of this issue requires user interaction in that a victim must open a malicious file. | 8.8 | More Details |

| CVE Number | Description | Base Score | Reference |
|---|---|---|---|
| CVE-2021-21101 | Adobe Illustrator version 25.2 (and earlier) is affected by an Out-of-bounds Write vulnerability when parsing a specially crafted file. An unauthenticated attacker could leverage this vulnerability to achieve arbitrary code execution in the context of the current user. Exploitation of this issue requires user interaction in that a victim must open a malicious file. | 8.8 | More Details |
| CVE-2021-29967 | Mozilla developers reported memory safety bugs present in Firefox 88 and Firefox ESR 78.11. 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 < 78.11, Firefox < 89, and Firefox ESR < 78.11. | 8.8 | More Details |
| CVE-2021-21099 | Adobe InDesign version 16.0 (and earlier) is affected by an Out-of-bounds Write vulnerability when parsing a crafted file. An unauthenticated attacker could leverage this vulnerability to achieve remote code execution in the context of the current user. Exploitation of this issue requires user interaction in that a victim must open a malicious file. | 8.8 | More Details |
| CVE-2021-21098 | Adobe InDesign version 16.0 (and earlier) is affected by an Out-of-bounds Write vulnerability when parsing a crafted file. An unauthenticated attacker could leverage this vulnerability to achieve remote code execution in the context of the current user. Exploitation of this issue requires user interaction in that a victim must open a malicious file. | 8.8 | More Details |
| CVE-2021-23995 | When Responsive Design Mode was enabled, it used references to objects that were previously freed. We presume that with enough effort this could have been exploited to run arbitrary code. This vulnerability affects Firefox ESR < 78.10, Thunderbird < 78.10, and Firefox < 88. | 8.8 | More Details |
| CVE-2021-21090 | Adobe InCopy version 16.0 (and earlier) is affected by an path traversal vulnerability when parsing a crafted file. An unauthenticated attacker could leverage this vulnerability to achieve remote code execution in the context of the current user. Exploitation of this issue requires user interaction in that a victim must open a malicious file. | 8.8 | More Details |
| CVE-2021-23997 | Due to unexpected data type conversions, a use-after-free could have occurred when interacting with the font cache. We presume that with enough effort this could have been exploited to run arbitrary code. This vulnerability affects Firefox < 88. | 8.8 | More Details |
| CVE-2021-33537 | In Weidmueller Industrial WLAN devices in multiple versions an exploitable remote code execution vulnerability exists in the iw_webs configuration parsing functionality. A specially crafted user name entry can cause an overflow of an error message buffer, resulting in remote code execution. An attacker can send commands while authenticated as a low privilege user to trigger this vulnerability. | 8.8 | More Details |
| CVE-2021-23999 | If a Blob URL was loaded through some unusual user interaction, it could have been loaded by the System Principal and granted additional privileges that should not be granted to web content. This vulnerability affects Firefox ESR < 78.10, Thunderbird < 78.10, and Firefox < 88. | 8.8 | More Details |
| CVE-2021-33538 | In Weidmueller Industrial WLAN devices in multiple versions an exploitable improper access control vulnerability exists in the iw_webs account settings functionality. A specially crafted user name entry can cause the overwrite of an existing user account password, resulting in remote shell access to the device as that user. An attacker can send commands while authenticated as a low privilege user to trigger this vulnerability. | 8.8 | More Details |
| CVE-2021-24002 | When a user clicked on an FTP URL containing encoded newline characters (%0A and %0D), the newlines would have been interpreted as such and allowed arbitrary commands to be sent to the FTP server. This vulnerability affects Firefox ESR < 78.10, Thunderbird < 78.10, and Firefox < 88. | 8.8 | More Details |
| CVE-2021-20740 | Hitachi Virtual File Platform Versions prior to 5.5.3-09 and Versions prior to 6.4.3-09, and NEC Storage M Series NAS Gateway Nh4a/Nh8a versions prior to FOS 5.5.3-08(NEC2.5.4a) and Nh4b/Nh8b, Nh4c/Nh8c versions prior to FOS 6.4.3-08(NEC3.4.2) allow remote authenticated attackers to execute arbitrary OS commands with root privileges via unspecified vectors. | 8.8 | More Details |
| CVE-2021-29966 | Mozilla developers reported memory safety bugs present in Firefox 88. 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 < 89. | 8.8 | More Details |
| CVE-2021-2322 | Vulnerability in OpenGrok (component: Web App). Versions that are affected are 1.6.7 and prior. Easily exploitable vulnerability allows low privileged attacker with network access via HTTPS to compromise OpenGrok. Successful attacks of this vulnerability can result in takeover of OpenGrok. CVSS 3.1 Base Score 8.8 (Confidentiality, Integrity and Availability impacts). CVSS Vector: (CVSS:3.1/AV:N/AC:L/PR:L/UI:N/S:U/C:H/I:H/A:H). | 8.8 | More Details |
| CVE-2021-29947 | Mozilla developers and community members reported memory safety bugs present in Firefox 87. 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 < 88. | 8.8 | More Details |
| CVE-2021-31586 | Accellion Kiteworks before 7.4.0 allows an authenticated user to perform SQL Injection via LDAPGroup Search. | 8.8 | More Details |
| CVE-2021-20102 | Machform prior to version 16 is vulnerable to cross-site request forgery due to a lack of CSRF tokens in place. | 8.8 | More Details |
| CVE-2020-21394 | SQL Injection vulnerability in Zhong Bang Technology Co., Ltd CRMEB mall system V2.60 and V3.1 via the tablename parameter in SystemDatabackup.php. | 8.8 | More Details |

| CVE Number | Description | Base Score | Reference |
|---|---|---|---|
| CVE-2020-21785 | In IBOS 4.5.4 Open, the database backup has Command Injection Vulnerability. | 8.8 | More Details |
| CVE-2021-34824 | Istio (1.8.x, 1.9.0-1.9.5 and 1.10.0-1.10.1) contains a remotely exploitable vulnerability where credentials specified in the Gateway and DestinationRule credentialName field can be accessed from different namespaces. | 8.8 | More Details |
| CVE-2020-17759 | An issue was found in the Evernote client for Windows 10, 7, and 2008 in the protocol handler. This enables attackers for arbitrary command execution if the user clicks on a specially crafted URL. AKA: WINNOTE-19941. | 8.8 | More Details |
| CVE-2021-23275 | The Windows Installation component of TIBCO Software Inc.'s TIBCO Enterprise Runtime for R - Server Edition, TIBCO Enterprise Runtime for R - Server Edition, TIBCO Enterprise Runtime for R - Server Edition, TIBCO Spotfire Analytics Platform for AWS Marketplace, TIBCO Spotfire Server, TIBCO Spotfire Server, TIBCO Spotfire Server, TIBCO Spotfire Statistics Services, TIBCO Spotfire Statistics Services, and TIBCO Spotfire Statistics Services contains a vulnerability that theoretically allows a low privileged attacker with local access on some versions of the Windows operating system to insert malicious software. The affected component can be abused to execute the malicious software inserted by the attacker with the elevated privileges of the component. This vulnerability results from a lack of access restrictions on certain files and/or folders in the installation. Affected releases are TIBCO Software Inc.'s TIBCO Enterprise Runtime for R - Server Edition: versions 1.2.4 and below, TIBCO Enterprise Runtime for R - Server Edition: versions 1.3.0 and 1.3.1, TIBCO Enterprise Runtime for R - Server Edition: versions 1.4.0, 1.5.0, and 1.6.0, TIBCO Spotfire Analytics Platform for AWS Marketplace: versions 11.3.0 and below, TIBCO Spotfire Server: versions 10.3.12 and below, TIBCO Spotfire Server: versions 10.4.0, 10.5.0, 10.6.0, 10.6.1, 10.7.0, 10.8.0, 10.8.1, 10.9.0, 10.10.0, 10.10.1, 10.10.2, 10.10.3, and 10.10.4, TIBCO Spotfire Server: versions 11.0.0, 11.1.0, 11.2.0, and 11.3.0, TIBCO Spotfire Statistics Services: versions 10.3.0 and below, TIBCO Spotfire Statistics Services: versions 10.10.0, 10.10.1, and 10.10.2, and TIBCO Spotfire Statistics Services: versions 11.1.0, 11.2.0, and 11.3.0. | 8.8 | More Details |
| CVE-2021-28830 | The TIBCO Spotfire Server and TIBCO Enterprise Runtime for R components of TIBCO Software Inc.'s TIBCO Enterprise Runtime for R - Server Edition, TIBCO Enterprise Runtime for R - Server Edition, TIBCO Enterprise Runtime for R - Server Edition, TIBCO Spotfire Analytics Platform for AWS Marketplace, TIBCO Spotfire Server, TIBCO Spotfire Server, TIBCO Spotfire Server, TIBCO Spotfire Statistics Services, TIBCO Spotfire Statistics Services, and TIBCO Spotfire Statistics Services contain a vulnerability that theoretically allows a low privileged attacker with local access on the Windows operating system to insert malicious software. The affected component can be abused to execute the malicious software inserted by the attacker with the elevated privileges of the component. This vulnerability results from the affected component searching for run-time artifacts outside of the installation hierarchy. Affected releases are TIBCO Software Inc.'s TIBCO Enterprise Runtime for R - Server Edition: versions 1.2.4 and below, TIBCO Enterprise Runtime for R - Server Edition: versions 1.3.0 and 1.3.1, TIBCO Enterprise Runtime for R - Server Edition: versions 1.4.0, 1.5.0, and 1.6.0, TIBCO Spotfire Analytics Platform for AWS Marketplace: versions 11.3.0 and below, TIBCO Spotfire Server: versions 10.3.12 and below, TIBCO Spotfire Server: versions 10.4.0, 10.5.0, 10.6.0, 10.6.1, 10.7.0, 10.8.0, 10.8.1, 10.9.0, 10.10.0, 10.10.1, 10.10.2, 10.10.3, and 10.10.4, TIBCO Spotfire Server: versions 11.0.0, 11.1.0, 11.2.0, and 11.3.0, TIBCO Spotfire Statistics Services: versions 10.3.0 and below, TIBCO Spotfire Statistics Services: versions 10.10.0, 10.10.1, and 10.10.2, and TIBCO Spotfire Statistics Services: versions 11.1.0, 11.2.0, and 11.3.0. | 8.8 | More Details |
| CVE-2021-29085 | Improper neutralization of special elements in output used by a downstream component ('Injection') vulnerability in file sharing management component in Synology DiskStation Manager (DSM) before 6.2.3-25426-3 allows remote attackers to read arbitrary files via unspecified vectors. | 8.6 | More Details |
| CVE-2020-23715 | Directory Traversal vulnerability in Webport CMS 1.19.10.17121 via the file parameter to file/download. | 8.6 | More Details |
| CVE-2021-32704 | DHIS 2 is an information system for data capture, management, validation, analytics and visualization. A SQL injection security vulnerability has been found in specific versions of DHIS2. This vulnerability affects the /api/trackedEntityInstances API endpoint in DHIS2 versions 2.34.4, 2.35.2, 2.35.3, 2.35.4, and 2.36.0. Earlier versions, such as 2.34.3 and 2.35.1 and all versions 2.33 and older are unaffected. The system is vulnerable to attack only from users that are logged in to DHIS2, and there is no known way of exploiting the vulnerability without first being logged in as a DHIS2 user. A successful exploit of this vulnerability could allow the malicious user to read, edit and delete data in the DHIS2 instance. There are no known exploits of the security vulnerabilities addressed by these patch releases. However, we strongly recommend that all DHIS2 implementations using versions 2.34, 2.35 and 2.36 install these patches as soon as possible. There is no straightforward known workaround for DHIS2 instances using the Tracker functionality other than upgrading the affected DHIS2 server to one of the patches in which this vulnerability has been fixed. For implementations which do NOT use Tracker functionality, it may be possible to block all network access to POST to the /api/trackedEntityInstance endpoint as a temporary workaround while waiting to upgrade. | 8.5 | More Details |
| CVE-2021-31838 | A command injection vulnerability in MVISION EDR (MVEDR) prior to 3.4.0 allows an authenticated MVEDR administrator to trigger the EDR client to execute arbitrary commands through PowerShell using the EDR functionality 'execute reaction'. | 8.4 | More Details |
| CVE-2021-1073 | NVIDIA GeForce Experience, all versions prior to 3.23, contains a vulnerability in the login flow when a user tries to log in by using a browser, while, at the same time, any other web page is loaded in other tabs of the same browser. In this situation, the web page can get access to the token of the user login session, leading to the possibility that the user’s account is compromised. This may lead to the targeted user’s data being accessed, altered, or lost. | 8.3 | More Details |
| CVE-2021-28570 | Adobe After Effects version 18.1 (and earlier) is affected by an Uncontrolled Search Path element vulnerability. An unauthenticated attacker could exploit this to to plant custom binaries and execute them with System permissions. Exploitation of this issue requires user interaction. | 8.3 | More Details |

| CVE Number | Description | Base Score | Reference |
|---|---|---|---|
| CVE-2021-22439 | There is a deserialization vulnerability in Huawei AnyOffice V200R006C10. An attacker can construct a specific request to exploit this vulnerability. Successfully exploiting this vulnerability, the attacker can execute remote malicious code injection and to control the device. | 8.1 | More Details |
| CVE-2020-4945 | IBM Db2 for Linux, UNIX and Windows (includes Db2 Connect Server) 11.5 could allow an authenticated user to overwrite arbirary files due to improper group permissions. IBM X-Force ID: 191945. | 8.1 | More Details |
| CVE-2021-20104 | Machform prior to version 16 is vulnerable to unauthenticated remote code execution due to insufficient sanitization of file attachments uploaded with forms through upload.php. | 8.1 | More Details |
| CVE-2021-29968 | When drawing text onto a canvas with WebRender disabled, an out of bounds read could occur. *This bug only affects Firefox on Windows. Other operating systems are unaffected.*. This vulnerability affects Firefox < 89.0.1. | 8.1 | More Details |
| CVE-2021-25923 | In OpenEMR, versions 5.0.0 to 6.0.0.1 are vulnerable to weak password requirements as it does not enforce a maximum password length limit. If a malicious user is aware of the first 72 characters of the victim user's password, he can leverage it to an account takeover. | 8.1 | More Details |
| CVE-2021-33895 | ETINET BACKBOX E4.09 and H4.09 mismanages password access control. When a user uses the User ID of the process running BBSV to login to the Backbox UI application, the system procedure (USER_AUTHENTICATE_) used for verifying the Password returns 0 (no error). The reason is that the user is not running the XYGate application. Hence, BBSV assumes the Password is correct. For H4.09, the affected version isT0954V04^AAO. For E4.09, the affected version is 22SEP2020. Note: If your current version is E4.10-16MAY2021 (version procedure T9999V04_16MAY2022_BPAKETI_10), a hotfix (FIXPAK-19OCT-2022) is available in version E4.10-19OCT2022. Resolution to CVE-2021-33895 in version E4.11-19OCT2022 | 8.1 | More Details |
| CVE-2021-28800 | A command injection vulnerability has been reported to affect QNAP NAS running legacy versions of QTS. If exploited, this vulnerability allows attackers to execute arbitrary commands in a compromised application. This issue affects: QNAP Systems Inc. QTS versions prior to 4.3.6.1663 Build 20210504; versions prior to 4.3.3.1624 Build 20210416. This issue does not affect: QNAP Systems Inc. QTS 4.5.3. QNAP Systems Inc. QuTS hero h4.5.3. QNAP Systems Inc. QuTScloud c4.5.5. | 8.1 | More Details |
| CVE-2021-25653 | A privilege escalation vulnerability was discovered in Avaya Aura Appliance Virtualization Platform Utilities (AVPU) that may potentially allow a local user to escalate privileges. Affects 8.0.0.0 through 8.1.3.1 versions of AVPU. | 8.0 | More Details |
| CVE-2021-32702 | The Auth0 Next.js SDK is a library for implementing user authentication in Next.js applications. Versions before and including `1.4.1` are vulnerable to reflected XSS. An attacker can execute arbitrary code by providing an XSS payload in the `error` query parameter which is then processed by the callback handler as an error message. You are affected by this vulnerability if you are using `@auth0/nextjs-auth0` version `1.4.1` or lower **unless** you are using custom error handling that does not return the error message in an HTML response. Upgrade to version `1.4.1` to resolve. The fix adds basic HTML escaping to the error message and it should not impact your users. | 8.0 | More Details |
| CVE-2021-25651 | A privilege escalation vulnerability was discovered in Avaya Aura Utility Services that may potentially allow a local user to escalate privileges. Affects all 7.x versions of Avaya Aura Utility Services | 8.0 | More Details |
| CVE-2021-27043 | An Arbitrary Address Write issue in the Autodesk DWG application can allow a malicious user to leverage the application to write in unexpected paths. In order to exploit this the attacker would need the victim to enable full page heap in the application. | 7.8 | More Details |
| CVE-2020-4609 | IBM Security Sevret Server (IBM Security Verify Privilege Manager 10.8.2) is vulnerable to a buffer overflow, caused by improper bounds checking. A local attacker could overflow a buffer and execute arbitrary code on the system or cause the system to crash. IBM X-Force ID: 184917. | 7.8 | More Details |
| CVE-2020-4610 | IBM Security Secret Server (IBM Security Verify Privilege Manager 10.8.2 ) could allow a local user to execute code due to improper integrity checks. IBM X-Force ID: 184919. | 7.8 | More Details |
| CVE-2021-29949 | When loading the shared library that provides the OTR protocol implementation, Thunderbird will initially attempt to open it using a filename that isn't distributed by Thunderbird. If a computer has already been infected with a malicious library of the alternative filename, and the malicious library has been copied to a directory that is contained in the search path for executable libraries, then Thunderbird will load the incorrect library. This vulnerability affects Thunderbird < 78.9.1. | 7.8 | More Details |
| CVE-2021-33002 | Opening a maliciously crafted project file may cause an out-of-bounds write, which may allow an attacker to execute arbitrary code. User interaction is require on the WebAccess HMI Designer (versions 2.1.9.95 and prior). | 7.8 | More Details |
| CVE-2021-33000 | Parsing a maliciously crafted project file may cause a heap-based buffer overflow, which may allow an attacker to perform arbitrary code execution. User interaction is required on the WebAccess HMI Designer (versions 2.1.9.95 and prior). | 7.8 | More Details |

| CVE Number | Description | Base Score | Reference |
|---|---|---|---|
| CVE-2021-3500 | A flaw was found in djvulibre-3.5.28 and earlier. A Stack overflow in function DJVU::DjVuDocument::get_djvu_file() via crafted djvu file may lead to application crash and other consequences. | 7.8 | More Details |
| CVE-2021-34185 | Miniaudio 0.10.35 has an integer-based buffer overflow caused by an out-of-bounds left shift in drwav_bytes_to_u32 in miniaudio.h | 7.8 | More Details |
| CVE-2021-27042 | A maliciously crafted DWG file can be used to write beyond the allocated buffer while parsing DWG files. The vulnerability exists because the application fails to handle a crafted DWG file, which causes an unhandled exception. An attacker can leverage this vulnerability to execute arbitrary code. | 7.8 | More Details |
| CVE-2021-27041 | A maliciously crafted DWG file can be used to write beyond the allocated buffer while parsing DWG files. This vulnerability can be exploited to execute arbitrary code | 7.8 | More Details |
| CVE-2021-32491 | A flaw was found in djvulibre-3.5.28 and earlier. An integer overflow in function render() in tools/ddjvu via crafted djvu file may lead to application crash and other consequences. | 7.8 | More Details |
| CVE-2021-32492 | A flaw was found in djvulibre-3.5.28 and earlier. An out of bounds read in function DJVU::DataPool::has_data() via crafted djvu file may lead to application crash and other consequences. | 7.8 | More Details |
| CVE-2021-32493 | A flaw was found in djvulibre-3.5.28 and earlier. A heap buffer overflow in function DJVU::GBitmap::decode() via crafted djvu file may lead to application crash and other consequences. | 7.8 | More Details |
| CVE-2021-35448 | Emote Interactive Remote Mouse 3.008 on Windows allows attackers to execute arbitrary programs as Administrator by using the Image Transfer Folder feature to navigate to cmd.exe. It binds to local ports to listen for incoming connections. | 7.8 | More Details |
| CVE-2021-32490 | A flaw was found in djvulibre-3.5.28 and earlier. An out of bounds write in function DJVU::filter_bv() via crafted djvu file may lead to application crash and other consequences. | 7.8 | More Details |
| CVE-2021-33004 | The affected product is vulnerable to memory corruption condition due to lack of proper validation of user supplied files, which may allow an attacker to execute arbitrary code. User interaction is required on the WebAccess HMI Designer (versions 2.1.9.95 and prior). | 7.8 | More Details |
| CVE-2021-31515 | This vulnerability allows remote attackers to execute arbitrary code on affected installations of Vector 35 Binary Ninja 2.3.2660 (Build ID 88f343c3). User interaction is required to exploit this vulnerability in that the target must visit a malicious page or open a malicious file. The specific flaw exists within the parsing of BNDB files. The issue results from the lack of proper validation of user-supplied data, which can result in a read past the end of an allocated data structure. An attacker can leverage this vulnerability to execute code in the context of the current process. Was ZDI-CAN-13668. | 7.8 | More Details |
| CVE-2021-31514 | This vulnerability allows remote attackers to execute arbitrary code on affected installations of OpenText Brava! Desktop Build 16.6.4.55. User interaction is required to exploit this vulnerability in that the target must visit a malicious page or open a malicious file. The specific flaw exists within the parsing of CGM files. The issue results from the lack of proper validation of user-supplied data, which can result in a write past the end of an allocated buffer. An attacker can leverage this vulnerability to execute code in the context of the current process. Was ZDI-CAN-13679. | 7.8 | More Details |
| CVE-2021-31508 | This vulnerability allows remote attackers to execute arbitrary code on affected installations of OpenText Brava! Desktop 16.6.3.84. User interaction is required to exploit this vulnerability in that the target must visit a malicious page or open a malicious file. The specific flaw exists within the parsing of DXF files. The issue results from the lack of proper validation of user-supplied data, which can result in a write past the end of an allocated buffer. An attacker can leverage this vulnerability to execute code in the context of the current process. Was ZDI-CAN-13306. | 7.8 | More Details |
| CVE-2021-33542 | Phoenix Contact Classic Automation Worx Software Suite in Version 1.87 and below is affected by a remote code execution vulnerability. Manipulated PC Worx or Config+ projects could lead to a remote code execution when unallocated memory is freed because of incompletely initialized data. The attacker needs to get access to an original bus configuration file (*.bcp) to be able to manipulate data inside. After manipulation the attacker needs to exchange the original file by the manipulated one on the application programming workstation. Availability, integrity, or confidentiality of an application programming workstation might be compromised by attacks using these vulnerabilities. Automated systems in operation which were programmed with one of the above-mentioned products are not affected. | 7.8 | More Details |
| CVE-2021-28691 | Guest triggered use-after-free in Linux xen-netback A malicious or buggy network PV frontend can force Linux netback to disable the interface and terminate the receive kernel thread associated with queue 0 in response to the frontend sending a malformed packet. Such kernel thread termination will lead to a use-after-free in Linux netback when the backend is destroyed, as the kernel thread associated with queue 0 will have already exited and thus the call to kthread_stop will be performed against a stale pointer. | 7.8 | More Details |

| CVE Number | Description | Base Score | Reference |
|---|---|---|---|
| CVE-2021-31509 | This vulnerability allows remote attackers to execute arbitrary code on affected installations of OpenText Brava! Desktop 16.6.3.84. User interaction is required to exploit this vulnerability in that the target must visit a malicious page or open a malicious file. The specific flaw exists within the parsing of DXF files. The issue results from the lack of proper validation of user-supplied data, which can result in a write past the end of an allocated buffer. An attacker can leverage this vulnerability to execute code in the context of the current process. Was ZDI-CAN-13309. | 7.8 | More Details |
| CVE-2021-31510 | This vulnerability allows remote attackers to execute arbitrary code on affected installations of OpenText Brava! Desktop Build 16.6.4.55. User interaction is required to exploit this vulnerability in that the target must visit a malicious page or open a malicious file. The specific flaw exists within the parsing of TIF files. The issue results from the lack of proper validation of user-supplied data, which can result in a read past the end of an allocated buffer. An attacker can leverage this vulnerability to execute code in the context of the current process. Was ZDI-CAN-13675. | 7.8 | More Details |
| CVE-2021-31511 | This vulnerability allows remote attackers to execute arbitrary code on affected installations of OpenText Brava! Desktop Build 16.6.4.55. User interaction is required to exploit this vulnerability in that the target must visit a malicious page or open a malicious file. The specific flaw exists within the parsing of PDF files. The issue results from the lack of proper validation of user-supplied data, which can result in a write past the end of an allocated buffer. An attacker can leverage this vulnerability to execute code in the context of the current process. Was ZDI-CAN-13676. | 7.8 | More Details |
| CVE-2021-31512 | This vulnerability allows remote attackers to execute arbitrary code on affected installations of OpenText Brava! Desktop Build 16.6.4.55. User interaction is required to exploit this vulnerability in that the target must visit a malicious page or open a malicious file. The specific flaw exists within the parsing of TIF files. The issue results from the lack of proper validation of user-supplied data, which can result in a read past the end of an allocated buffer. An attacker can leverage this vulnerability to execute code in the context of the current process. Was ZDI-CAN-13677. | 7.8 | More Details |
| CVE-2021-31513 | This vulnerability allows remote attackers to execute arbitrary code on affected installations of OpenText Brava! Desktop Build 16.6.4.55. User interaction is required to exploit this vulnerability in that the target must visit a malicious page or open a malicious file. The specific flaw exists within the parsing of BMP files. The issue results from the lack of proper validation of user-supplied data, which can result in a write past the end of an allocated buffer. An attacker can leverage this vulnerability to execute code in the context of the current process. Was ZDI-CAN-13678. | 7.8 | More Details |
| CVE-2021-31507 | This vulnerability allows remote attackers to execute arbitrary code on affected installations of OpenText Brava! Desktop 16.6.3.84. User interaction is required to exploit this vulnerability in that the target must visit a malicious page or open a malicious file. The specific flaw exists within the parsing of CGM files. The issue results from the lack of proper validation of the length of user-supplied data prior to copying it to a stack-based buffer. An attacker can leverage this vulnerability to execute code in the context of the current process. Was ZDI-CAN-12653. | 7.8 | More Details |
| CVE-2021-31516 | This vulnerability allows remote attackers to execute arbitrary code on affected installations of Vector 35 Binary Ninja 2.3.2660 (Build ID 88f343c3). User interaction is required to exploit this vulnerability in that the target must visit a malicious page or open a malicious file. The specific flaw exists within the parsing of BNDB files. The issue results from the lack of validating the existence of an object prior to performing operations on the object. An attacker can leverage this vulnerability to execute code in the context of the current process. Was ZDI-CAN-13670. | 7.8 | More Details |
| CVE-2021-35523 | Securepoint SSL VPN Client v2 before 2.0.32 on Windows has unsafe configuration handling that enables local privilege escalation to NT AUTHORITY\SYSTEM. A non-privileged local user can modify the OpenVPN configuration stored under "%APPDATA%\Securepoint SSL VPN" and add a external script file that is executed as privileged user. | 7.8 | More Details |
| CVE-2021-28586 | After Effects version 18.0 (and earlier) are affected by an out-of-bounds write vulnerability that could result in arbitrary code execution in the context of the current user. Exploitation of this issue requires user interaction in that a victim must open a malicious file. | 7.8 | More Details |
| CVE-2021-21871 | A memory corruption vulnerability exists in the DMG File Format Handler functionality of PowerISO 7.9. A specially crafted DMG file can lead to an out-of-bounds write. An attacker can provide a malicious file to trigger this vulnerability. The vendor fixed it in a bug-release of the current version. | 7.8 | More Details |
| CVE-2021-21999 | VMware Tools for Windows (11.x.y prior to 11.2.6), VMware Remote Console for Windows (12.x prior to 12.0.1) , VMware App Volumes (2.x prior to 2.18.10 and 4 prior to 2103) contain a local privilege escalation vulnerability. An attacker with normal access to a virtual machine may exploit this issue by placing a malicious file renamed as `openssl.cnf' in an unrestricted directory which would allow code to be executed with elevated privileges. | 7.8 | More Details |
| CVE-2021-20745 | Inkdrop versions prior to v5.3.1 allows an attacker to execute arbitrary OS commands on the system where it runs by loading a file or code snippet containing an invalid iframe into Inkdrop. | 7.8 | More Details |
| CVE-2021-25650 | A privilege escalation vulnerability was discovered in Avaya Aura Utility Services that may potentially allow a local user to execute specially crafted scripts as a privileged user. Affects all 7.x versions of Avaya Aura Utility Services | 7.7 | More Details |
| CVE-2021-31530 | Zoho ManageEngine ServiceDesk Plus MSP before 10522 is vulnerable to Information Disclosure. | 7.5 | More Details |
| CVE-2021-29703 | Db2 for Linux, UNIX and Windows (includes Db2 Connect Server) is vulnerable to a denial of service as the server terminates abnormally when executing a specially crafted SELECT statement. IBM X-Force ID: 200659. | 7.5 | More Details |

| CVE Number | Description | Base Score | Reference |
|---|---|---|---|
| CVE-2021-22119 | Spring Security versions 5.5.x prior to 5.5.1, 5.4.x prior to 5.4.7, 5.3.x prior to 5.3.10 and 5.2.x prior to 5.2.11 are susceptible to a Denial-of-Service (DoS) attack via the initiation of the Authorization Request in an OAuth 2.0 Client Web and WebFlux application. A malicious user or attacker can send multiple requests initiating the Authorization Request for the Authorization Code Grant, which has the potential of exhausting system resources using a single session or multiple sessions. | 7.5 | More Details |
| CVE-2021-32717 | Shopware is an open source eCommerce platform. In versions prior to 6.4.1.1 private files publicly accessible with Cloud Storage providers when the hashed URL is known. Users are recommend to first change their configuration to set the correct visibility according to the documentation. The visibility must be at the same level as `type`. When the Storage is saved on Amazon AWS we recommending disabling public access to the bucket containing the private files: https://docs.aws.amazon.com/AmazonS3/latest/userguide/access-control-block-public-access.html. Otherwise, update to Shopware 6.4.1.1 or install or update the Security plugin (https://store.shopware.com/en/detail/index/sArticle/518463/number/Swag136939272659) and run the command `./bin/console s3:set-visibility` to correct your cloud file visibilities. | 7.5 | More Details |
| CVE-2021-33541 | Phoenix Contact Classic Line Controllers ILC1x0 and ILC1x1 in all versions/variants are affected by a Denial-of-Service vulnerability. The communication protocols and device access do not feature authentication measures. Remote attackers can use specially crafted IP packets to cause a denial of service on the PLC's network communication module. A successful attack stops all network communication. To restore the network connectivity the device needs to be restarted. The automation task is not affected. | 7.5 | More Details |
| CVE-2021-34549 | An issue was discovered in Tor before 0.4.6.5, aka TROVE-2021-005. Hashing is mishandled for certain retrieval of circuit data. Consequently. an attacker can trigger the use of an attacker-chosen circuit ID to cause algorithm inefficiency. | 7.5 | More Details |
| CVE-2021-31160 | Zoho ManageEngine ServiceDesk Plus MSP before 10521 allows an attacker to access internal data. | 7.5 | More Details |
| CVE-2021-33503 | An issue was discovered in urllib3 before 1.26.5. When provided with a URL containing many @ characters in the authority component, the authority regular expression exhibits catastrophic backtracking, causing a denial of service if a URL were passed as a parameter or redirected to via an HTTP redirect. | 7.5 | More Details |
| CVE-2021-29157 | Dovecot before 2.3.15 allows ../ Path Traversal. An attacker with access to the local filesystem can trick OAuth2 authentication into using an HS256 validation key from an attacker-controlled location. This occurs during use of local JWT validation with the posix fs driver. | 7.5 | More Details |
| CVE-2021-21083 | AEM's Cloud Service offering, as well as versions 6.5.7.0 (and below), 6.4.8.3 (and below) and 6.3.3.8 (and below) are affected by an Improper Access Control vulnerability. An unauthenticated attacker could leverage this vulnerability to cause an application denial-of-service in the context of the current user. | 7.5 | More Details |
| CVE-2021-33536 | In Weidmueller Industrial WLAN devices in multiple versions an exploitable denial-of-service vulnerability exists in ServiceAgent functionality. A specially crafted packet can cause an integer underflow, triggering a large memcpy that will access unmapped or out-of-bounds memory. An attacker can send this packet while unauthenticated to trigger this vulnerability. | 7.5 | More Details |
| CVE-2021-28583 | Magento versions 2.4.2 (and earlier), 2.4.1-p1 (and earlier) and 2.3.6-p1 (and earlier) are affected by a Violation of Secure Design Principles vulnerability in RMA PDF filename formats. Successful exploitation could allow an attacker to get unauthorized access to restricted resources. | 7.5 | More Details |
| CVE-2021-35299 | Incorrect Access Control in Zammad 1.0.x up to 4.0.0 allows attackers to obtain sensitive information via email connection configuration probing. | 7.5 | More Details |
| CVE-2021-33529 | In Weidmueller Industrial WLAN devices in multiple versions the usage of hard-coded cryptographic keys within the service agent binary allows for the decryption of captured traffic across the network from or to the device. | 7.5 | More Details |
| CVE-2021-21005 | In Phoenix Contact FL SWITCH SMCS series products in multiple versions if an attacker sends a hand-crafted TCP-Packet with the Urgent-Flag set and the Urgent-Pointer set to 0, the network stack will crash. The device needs to be rebooted afterwards. | 7.5 | More Details |
| CVE-2020-7871 | A vulnerability of Helpcom could allow an unauthenticated attacker to execute arbitrary command. This vulnerability exists due to insufficient validation of the parameter. This issue affects: Cnesty Helpcom 10.0 versions prior to. | 7.5 | More Details |
| CVE-2021-21002 | In Phoenix Contact FL COMSERVER UNI in versions < 2.40 a invalid Modbus exception response can lead to a temporary denial of service. | 7.5 | More Details |
| CVE-2021-34548 | An issue was discovered in Tor before 0.4.6.5, aka TROVE-2021-003. An attacker can forge RELAY_END or RELAY_RESOLVED to bypass the intended access control for ending a stream. | 7.5 | More Details |
| CVE-2021-22545 | An attacker can craft a specific IdaPro *.i64 file that will cause the BinDiff plugin to load an invalid memory offset. This can allow the attacker to control the instruction pointer and execute arbitrary code. It is recommended to upgrade BinDiff 7 | 7.5 | More Details |

| CVE Number | Description | Base Score | Reference |
|---|---|---|---|
| CVE-2021-27577 | Incorrect handling of url fragment vulnerability of Apache Traffic Server allows an attacker to poison the cache. This issue affects Apache Traffic Server 7.0.0 to 7.1.12, 8.0.0 to 8.1.1, 9.0.0 to 9.0.1. | 7.5 | More Details |
| CVE-2021-32565 | Invalid values in the Content-Length header sent to Apache Traffic Server allows an attacker to smuggle requests. This issue affects Apache Traffic Server 7.0.0 to 7.1.12, 8.0.0 to 8.1.1, 9.0.0 to 9.0.1. | 7.5 | More Details |
| CVE-2021-34550 | An issue was discovered in Tor before 0.4.6.5, aka TROVE-2021-006. The v3 onion service descriptor parsing allows out-of-bounds memory access, and a client crash, via a crafted onion service descriptor | 7.5 | More Details |
| CVE-2021-29084 | Improper neutralization of special elements in output used by a downstream component ('Injection') vulnerability in Security Advisor report management component in Synology DiskStation Manager (DSM) before 6.2.3-25426-3 allows remote attackers to read arbitrary files via unspecified vectors. | 7.5 | More Details |
| CVE-2021-35941 | Western Digital WD My Book Live (2.x and later) and WD My Book Live Duo (all versions) have an administrator API that can perform a system factory restore without authentication, as exploited in the wild in June 2021, a different vulnerability than CVE-2018-18472. | 7.5 | More Details |
| CVE-2021-20019 | A vulnerability in SonicOS where the HTTP server response leaks partial memory by sending a crafted HTTP request, this can potentially lead to an internal sensitive data disclosure vulnerability. | 7.5 | More Details |
| CVE-2021-29087 | Improper limitation of a pathname to a restricted directory ('Path Traversal') vulnerability in webapi component in Synology DiskStation Manager (DSM) before 6.2.3-25426-3 allows remote attackers to write arbitrary files via unspecified vectors. | 7.5 | More Details |
| CVE-2021-21737 | A smart STB product of ZTE is impacted by a permission and access control vulnerability. Due to insufficient protection of system application, attackers could use this vulnerability to tamper with the system desktop and affect system customization functions. This affects: ZXV10 B860H V5.0, V83011303.0010, V83011303.0016 | 7.5 | More Details |
| CVE-2021-29952 | When Web Render components were destructed, a race condition could have caused undefined behavior, and we presume that with enough effort may have been exploitable to run arbitrary code. This vulnerability affects Firefox < 88.0.1 and Firefox for Android < 88.1.3. | 7.5 | More Details |
| CVE-2021-29950 | Thunderbird unprotects a secret OpenPGP key prior to using it for a decryption, signing or key import task. If the task runs into a failure, the secret key may remain in memory in its unprotected state. This vulnerability affects Thunderbird < 78.8.1. | 7.5 | More Details |
| CVE-2021-29620 | Report portal is an open source reporting and analysis framework. Starting from version 3.1.0 of the service-api XML parsing was introduced. Unfortunately the XML parser was not configured properly to prevent XML external entity (XXE) attacks. This allows a user to import a specifically-crafted XML file which imports external Document Type Definition (DTD) file with external entities for extraction of secrets from Report Portal service-api module or server-side request forgery. This will be resolved in the 5.4.0 release. | 7.5 | More Details |
| CVE-2021-35041 | The blockchain node in FISCO-BCOS V2.7.2 may have a bug when dealing with unformatted packet and lead to a crash. A malicious node can send a packet continuously. The packet is in an incorrect format and cannot be decoded by the node correctly. As a result, the node may consume the memory sustainably and crash. More details are shown at: https://github.com/FISCO-BCOS/FISCO-BCOS/issues/1951 | 7.5 | More Details |
| CVE-2021-21004 | In Phoenix Contact FL SWITCH SMCS series products in multiple versions an attacker may insert malicious code via LLDP frames into the web-based management which could then be executed by the client. | 7.4 | More Details |
| CVE-2021-32723 | Prism is a syntax highlighting library. Some languages before 1.24.0 are vulnerable to Regular Expression Denial of Service (ReDoS). When Prism is used to highlight untrusted (user-given) text, an attacker can craft a string that will take a very very long time to highlight. This problem has been fixed in Prism v1.24. As a workaround, do not use ASCIIDoc or ERB to highlight untrusted text. Other languages are not affected and can be used to highlight untrusted text. | 7.4 | More Details |
| CVE-2021-1134 | A vulnerability in the Cisco Identity Services Engine (ISE) integration feature of the Cisco DNA Center Software could allow an unauthenticated, remote attacker to gain unauthorized access to sensitive data. The vulnerability is due to an incomplete validation of the X.509 certificate used when establishing a connection between DNA Center and an ISE server. An attacker could exploit this vulnerability by supplying a crafted certificate and could then intercept communications between the ISE and DNA Center. A successful exploit could allow the attacker to view and alter sensitive information that the ISE maintains about clients that are connected to the network. | 7.4 | More Details |
| CVE-2021-33540 | In certain devices of the Phoenix Contact AXL F BK and IL BK product families an undocumented password protected FTP access to the root directory exists. | 7.3 | More Details |
| CVE-2021-23399 | This affects all versions of package wincred. If attacker-controlled user input is given to the getCredential function, it is possible for an attacker to execute arbitrary commands. This is due to use of the child_process exec function without input sanitization. | 7.3 | More Details |

| CVE Number | Description | Base Score | Reference |
|---|---|---|---|
| CVE-2021-21084 | AEM's Cloud Service offering, as well as versions 6.5.7.0 (and below), 6.4.8.3 (and below) and 6.3.3.8 (and below) are affected by a stored Cross-Site Scripting (XSS) vulnerability that could be abused by an attacker to inject malicious scripts into vulnerable form fields. Malicious JavaScript may be executed in a victim's browser when they browse to the page containing the vulnerable field. | 7.3 | More Details |
| CVE-2021-21572 | Dell BIOSConnect feature contains a buffer overflow vulnerability. An authenticated malicious admin user with local access to the system may potentially exploit this vulnerability to run arbitrary code and bypass UEFI restrictions. | 7.2 | More Details |
| CVE-2021-33539 | In Weidmueller Industrial WLAN devices in multiple versions an exploitable authentication bypass vulnerability exists in the hostname processing. A specially configured device hostname can cause the device to interpret selected remote traffic as local traffic, resulting in a bypass of web authentication. An attacker can send authenticated SNMP requests to trigger this vulnerability. | 7.2 | More Details |
| CVE-2021-21573 | Dell BIOSConnect feature contains a buffer overflow vulnerability. An authenticated malicious admin user with local access to the system may potentially exploit this vulnerability to run arbitrary code and bypass UEFI restrictions. | 7.2 | More Details |
| CVE-2021-21574 | Dell BIOSConnect feature contains a buffer overflow vulnerability. An authenticated malicious admin user with local access to the system may potentially exploit this vulnerability to run arbitrary code and bypass UEFI restrictions. | 7.2 | More Details |
| CVE-2021-33534 | In Weidmueller Industrial WLAN devices in multiple versions an exploitable command injection vulnerability exists in the hostname functionality. A specially crafted entry to network configuration information can cause execution of arbitrary system commands, resulting in full control of the device. An attacker can send various requests while authenticated as a high privilege user to trigger this vulnerability. | 7.2 | More Details |
| CVE-2021-28976 | Remote Code Execution vulnerability in GetSimpleCMS before 3.3.16 in admin/upload.php via phar filess. | 7.2 | More Details |
| CVE-2021-29964 | A locally-installed hostile program could send `WM_COPYDATA` messages that Firefox would process incorrectly, leading to an out-of-bounds read. *This bug only affects Firefox on Windows. Other operating systems are unaffected.*. This vulnerability affects Thunderbird < 78.11, Firefox < 89, and Firefox ESR < 78.11. | 7.1 | More Details |
| CVE-2020-7862 | A vulnerability in agent program of HelpU remote control solution could allow an authenticated remote attacker to execute arbitrary commands This vulnerability is due to insufficient input santization when communicating customer process. | 7.0 | More Details |
| CVE-2021-29479 | Ratpack is a toolkit for creating web applications. In versions prior to 1.9.0, a user supplied `X-Forwarded-Host` header can be used to perform cache poisoning of a cache fronting a Ratpack server if the cache key does not include the `X-Forwarded-Host` header as a cache key. Users are only vulnerable if they do not configure a custom `PublicAddress` instance. For versions prior to 1.9.0, by default, Ratpack utilizes an inferring version of `PublicAddress` which is vulnerable. This can be used to perform redirect cache poisoning where an attacker can force a cached redirect to redirect to their site instead of the intended redirect location. The vulnerability was patched in Ratpack 1.9.0. As a workaround, ensure that `ServerConfigBuilder::publicAddress` correctly configures the server in production. | 7.0 | More Details |
| CVE-2021-28556 | Magento versions 2.4.2 (and earlier), 2.4.1-p1 (and earlier) and 2.3.6-p1 (and earlier) are affected by a DOM-based Cross-Site Scripting vulnerability on mage-messages cookies. Successful exploitation could lead to arbitrary JavaScript execution by an unauthenticated attacker. User interaction is required for successful exploitation. | 6.9 | More Details |
| CVE-2021-23991 | If a Thunderbird user has previously imported Alice's OpenPGP key, and Alice has extended the validity period of her key, but Alice's updated key has not yet been imported, an attacker may send an email containing a crafted version of Alice's key with an invalid subkey, Thunderbird might subsequently attempt to use the invalid subkey, and will fail to send encrypted email to Alice. This vulnerability affects Thunderbird < 78.9.1. | 6.8 | More Details |
| CVE-2021-31505 | This vulnerability allows attackers with physical access to escalate privileges on affected installations of Arlo Q Plus 1.9.0.3_278. Authentication is not required to exploit this vulnerability. The specific flaw exists within the SSH service. The device can be booted into a special operation mode where hard-coded credentials are accepted for SSH authentication. An attacker can leverage this vulnerability to escalate privileges and execute arbitrary code in the context of root. Was ZDI-CAN-12890. | 6.8 | More Details |
| CVE-2021-20100 | Nessus Agent 8.2.4 and earlier for Windows were found to contain multiple local privilege escalation vulnerabilities which could allow an authenticated, local administrator to run specific Windows executables as the Nessus host. This is different than CVE-2021-20099. | 6.7 | More Details |
| CVE-2021-20099 | Nessus Agent 8.2.4 and earlier for Windows were found to contain multiple local privilege escalation vulnerabilities which could allow an authenticated, local administrator to run specific Windows executables as the Nessus host. This is different than CVE-2021-20100. | 6.7 | More Details |
| CVE-2021-20079 | Nessus versions 8.13.2 and earlier were found to contain a privilege escalation vulnerability which could allow a Nessus administrator user to upload a specially crafted file that could lead to gaining administrator privileges on the Nessus host. | 6.7 | More Details |
| CVE-2021-31585 | Accellion Kiteworks before 7.3.1 allows a user with Admin privileges to escalate their privileges by generating SSH passwords that allow local access. | 6.7 | More Details |

| CVE Number | Description | Base Score | Reference |
|---|---|---|---|
| CVE-2021-29951 | The Mozilla Maintenance Service granted SERVICE_START access to BUILTIN\Users which, in a domain network, grants normal remote users access to start or stop the service. This could be used to prevent the browser update service from operating (if an attacker spammed the 'Stop' command); but also exposed attack surface in the maintenance service. *Note: This issue only affected Windows operating systems older than Win 10 build 1709. Other operating systems are unaffected.*. This vulnerability affects Thunderbird < 78.10.1, Firefox < 87, and Firefox ESR < 78.10.1. | 6.5 | More Details |
| CVE-2021-20573 | IBM Security Identity Manager Adapters 6.0 and 7.0 are vulnerable to a heap-based buffer overflow, caused by improper bounds checking. A remote authenticated attacker could overflow the and cause the server to crash. IBM X-Force ID: 199249. | 6.5 | More Details |
| CVE-2021-28690 | x86: TSX Async Abort protections not restored after S3 This issue relates to the TSX Async Abort speculative security vulnerability. Please see https://xenbits.xen.org/xsa/advisory-305.html for details. Mitigating TAA by disabling TSX (the default and preferred option) requires selecting a non-default setting in MSR_TSX_CTRL. This setting isn't restored after S3 suspend. | 6.5 | More Details |
| CVE-2021-20572 | IBM Security Identity Manager Adapters 6.0 and 7.0 are vulnerable to a stack-based buffer overflow, caused by improper bounds checking. A remote authenticated attacker could overflow the and cause the server to crash. IBM X-Force ID: 199247. | 6.5 | More Details |
| CVE-2021-20494 | IBM Security Identity Manager Adapters 6.0 and 7.0 are vulnerable to a heap based buffer overflow, caused by improper bounds. An authenticared user could overflow the buffer and cause the service to crash. IBM X-Force ID: 197882. | 6.5 | More Details |
| CVE-2021-20579 | IBM Db2 for Linux, UNIX and Windows (includes Db2 Connect Server) 9.7, 10.1, 10.5, 11.1, and 11.5 could allow a user who can create a view or inline SQL function to obtain sensitive information when AUTO_REVAL is set to DEFFERED_FORCE. IBM X-Force ID: 199283. | 6.5 | More Details |
| CVE-2021-32722 | GlobalNewFiles is a mediawiki extension. Versions prior to 48be7adb70568e20e961ea1cb70904454a671b1d are affected by an uncontrolled resource consumption vulnerability. A large amount of page moves within a short space of time could overwhelm Database servers due to improper handling of load balancing and a lack of an appropriate index. As a workaround, one may avoid use of the extension unless additional rate limit at the MediaWiki level or via PoolCounter / MySQL is enabled. A patch is available in version 48be7adb70568e20e961ea1cb70904454a671b1d. | 6.5 | More Details |
| CVE-2020-17753 | An issue was discovered in function addMeByRC in the smart contract implementation for RC, an Ethereum token, allows attackers to transfer an arbitrary amount of tokens to an arbitrary address. | 6.5 | More Details |
| CVE-2020-15303 | Infoblox NIOS before 8.5.2 allows entity expansion during an XML upload operation, a related issue to CVE-2003-1564. | 6.5 | More Details |
| CVE-2021-29945 | The WebAssembly JIT could miscalculate the size of a return type, which could lead to a null read and result in a crash. *Note: This issue only affected x86-32 platforms. Other platforms are unaffected.*. This vulnerability affects Firefox ESR < 78.10, Thunderbird < 78.10, and Firefox < 88. | 6.5 | More Details |
| CVE-2021-23998 | Through complicated navigations with new windows, an HTTP page could have inherited a secure lock icon from an HTTPS page. This vulnerability affects Firefox ESR < 78.10, Thunderbird < 78.10, and Firefox < 88. | 6.5 | More Details |
| CVE-2021-29481 | Ratpack is a toolkit for creating web applications. In versions prior to 1.9.0, the default configuration of client side sessions results in unencrypted, but signed, data being set as cookie values. This means that if something sensitive goes into the session, it could be read by something with access to the cookies. For this to be a vulnerability, some kind of sensitive data would need to be stored in the session and the session cookie would have to leak. For example, the cookies are not configured with httpOnly and an adjacent XSS vulnerability within the site allowed capture of the cookies. As of version 1.9.0, a securely randomly generated signing key is used. As a workaround, one may supply an encryption key, as per the documentation recommendation. | 6.5 | More Details |
| CVE-2021-23996 | By utilizing 3D CSS in conjunction with Javascript, content could have been rendered outside the webpage's viewport, resulting in a spoofing attack that could have been used for phishing or other attacks on a user. This vulnerability affects Firefox < 88. | 6.5 | More Details |
| CVE-2021-35050 | User credentials stored in a recoverable format within Fidelis Network and Deception CommandPost. In the event that an attacker gains access to the CommandPost, these values could be decoded and used to login to the application. The vulnerability is present in Fidelis Network and Deception versions prior to 9.3.3. This vulnerability has been addressed in version 9.3.3 and subsequent versions. | 6.5 | More Details |
| CVE-2021-23993 | An attacker may perform a DoS attack to prevent a user from sending encrypted email to a correspondent. If an attacker creates a crafted OpenPGP key with a subkey that has an invalid self signature, and the Thunderbird user imports the crafted key, then Thunderbird may try to use the invalid subkey, but the RNP library rejects it from being used, causing encryption to fail. This vulnerability affects Thunderbird < 78.9.1. | 6.5 | More Details |
| CVE-2021-29777 | IBM Db2 for Linux, UNIX and Windows (includes Db2 Connect Server) 9.7, 10.1, 10.5, 11.1, and 11.5, under specific circumstance of a table being dropped while being accessed in another session, could allow an authenticated user to cause a denial of srevice IBM X-Force ID: 203031. | 6.5 | More Details |
| CVE-2021-28563 | Magento versions 2.4.2 (and earlier), 2.4.1-p1 (and earlier) and 2.3.6-p1 (and earlier) are affected by an Improper Authorization vulnerability via the 'Create Customer' endpoint. Successful exploitation could lead to unauthorized modification of customer data by an unauthenticated attacker. Access to the admin console is required for successful exploitation. | 6.5 | More Details |

| CVE Number | Description | Base Score | Reference |
|---|---|---|---|
| CVE-2020-7870 | A memory corruption vulnerability exists when ezPDF improperly handles the parameter. This vulnerability exists due to insufficient validation of the parameter. | 6.4 | More Details |
| CVE-2021-23400 | The package nodemailer before 6.6.1 are vulnerable to HTTP Header Injection if unsanitized user input that may contain newlines and carriage returns is passed into an address object. | 6.3 | More Details |
| CVE-2021-25654 | An arbitrary code execution vulnerability was discovered in Avaya Aura Device Services that may potentially allow a local user to execute specially crafted scripts. Affects 7.0 through 8.1.4.0 versions of Avaya Aura Device Services. | 6.2 | More Details |
| CVE-2021-35513 | Mermaid before 8.11.0 allows XSS when the antiscript feature is used. | 6.1 | More Details |
| CVE-2021-20751 | Cross-site scripting vulnerability in EC-CUBE EC-CUBE 4.0.0 to 4.0.5-p1 (EC-CUBE 4 series) allows a remote attacker to inject an arbitrary script by leading an administrator or a user to a specially crafted page and to perform a specific operation. | 6.1 | More Details |
| CVE-2020-21142 | Cross Site Scripting (XSS) vulnerabilty in IPFire 2.23 via the IPfire web UI in the mail.cgi. | 6.1 | More Details |
| CVE-2021-20750 | Cross-site scripting vulnerability in EC-CUBE EC-CUBE 3.0.0 to 3.0.18-p2 (EC-CUBE 3 series) and EC-CUBE 4.0.0 to 4.0.5-p1 (EC-CUBE 4 series) allows a remote attacker to inject an arbitrary script by leading an administrator or a user to a specially crafted page and to perform a specific operation. | 6.1 | More Details |
| CVE-2021-35298 | Cross Site Scripting (XSS) in Zammad 1.0.x up to 4.0.0 allows remote attackers to execute arbitrary web script or HTML via multiple models that contain a 'note' field to store additional information. | 6.1 | More Details |
| CVE-2020-22609 | Cross Site Scripting (XSS) vulnerability in Enhancesoft osTicket before v1.12.6 via the queue-name parameter in include/class.queue.php. | 6.1 | More Details |
| CVE-2021-35303 | Cross Site Scripting (XSS) in Zammad 1.0.x up to 4.0.0 allows remote attackers to execute arbitrary web script or HTML via the User Avatar attribute. | 6.1 | More Details |
| CVE-2020-22608 | Cross Site Scripting vulnerability in Enhancesoft osTicket before v1.12.6 via the queue-name parameter to include/ajax.search.php. | 6.1 | More Details |
| CVE-2020-22607 | Cross Site Scripting vulnerabilty in LimeSurvey 4.1.11+200316 via the (1) name and (2) description parameters in application/controllers/admin/PermissiontemplatesController.php. | 6.1 | More Details |
| CVE-2020-20640 | Cross Site Scripting (XSS) vulnerability in ECShop 4.0 due to security filtering issues, in the user.php file, we can use the html entity encoding to bypass the security policy of the safety.php file, triggering the xss vulnerability. | 6.1 | More Details |
| CVE-2021-20101 | Machform prior to version 16 is vulnerable to HTTP host header injection due to improperly validated host headers. This could cause a victim to receive malformed content. | 6.1 | More Details |
| CVE-2021-29953 | A malicious webpage could have forced a Firefox for Android user into executing attacker-controlled JavaScript in the context of another domain, resulting in a Universal Cross-Site Scripting vulnerability. *Note: This issue only affected Firefox for Android. Other operating systems are unaffected. Further details are being temporarily withheld to allow users an opportunity to update.*. This vulnerability affects Firefox < 88.0.1 and Firefox for Android < 88.1.3. | 6.1 | More Details |
| CVE-2020-18659 | Cross Site Scripting vulnerability in GetSimpleCMS <=3.3.15 via the (1) sitename, (2) username, and (3) email parameters to /admin/setup.php | 6.1 | More Details |
| CVE-2021-35438 | phpIPAM 1.4.3 allows Reflected XSS via app/dashboard/widgets/ipcalc-result.php and app/tools/ip-calculator/result.php of the IP calculator. | 6.1 | More Details |

| CVE Number | Description | Base Score | Reference |
|---|---|---|---|
| CVE-2021-3314 | Oracle GlassFish Server 3.1.2.18 and below allows /common/logViewer/logViewer.jsf XSS. A malicious user can cause an administrator user to supply dangerous content to the vulnerable page, which is then reflected back to the user and executed by the web browser. The most common mechanism for delivering malicious content is to include it as a parameter in a URL that is posted publicly or e-mailed directly to victims. NOTE: This vulnerability only affects products that are no longer supported by the maintainer | 6.1 | More Details |
| CVE-2021-20103 | Machform prior to version 16 is vulnerable to stored cross-site scripting due to insufficient sanitization of file attachments uploaded with forms through upload.php. | 6.1 | More Details |
| CVE-2021-20105 | Machform prior to version 16 is vulnerable to an open redirect in Safari_init.php due to an improperly sanitized 'ref' parameter. | 6.1 | More Details |
| CVE-2020-18657 | Cross Site Scripting (XSS) vulnerability in GetSimpleCMS <= 3.3.15 in admin/changedata.php via the redirect_url parameter and the headers_sent function. | 6.1 | More Details |
| CVE-2020-18658 | Cross Site Scriptiong (XSS) vulnerability in GetSimpleCMS <=3.3.15 via the timezone parameter to settings.php. | 6.1 | More Details |
| CVE-2021-29944 | Lack of escaping allowed HTML injection when a webpage was viewed in Reader View. While a Content Security Policy prevents direct code execution, HTML injection is still possible. *Note: This issue only affected Firefox for Android. Other operating systems are unaffected.*. This vulnerability affects Firefox < 88. | 6.1 | More Details |
| CVE-2020-23962 | A cross site scripting (XSS) vulnerability in Catfish CMS 4.9.90 allows attackers to execute arbitrary web scripts or HTML via a crafted payload entered into the "announcement_gonggao" parameter. | 6.1 | More Details |
| CVE-2020-18660 | GetSimpleCMS <=3.3.15 has an open redirect in admin/changedata.php via the redirect function to the url parameter. | 6.1 | More Details |
| CVE-2021-23398 | All versions of package react-bootstrap-table are vulnerable to Cross-site Scripting (XSS) via the dataFormat parameter. The problem is triggered when an invalid React element is returned, leading to dangerouslySetInnerHTML being used, which does not sanitize the output. | 6.1 | More Details |
| CVE-2021-34254 | Umbraco CMS before 7.15.7 is vulnerable to Open Redirection due to insufficient url sanitization on booting.aspx. | 6.1 | More Details |
| CVE-2020-18066 | Cross Site Scripting vulnerability in ZrLog 2.1.0 via the (1) userName and (2) email parameters in post/addComment. | 6.1 | More Details |
| CVE-2021-33348 | An issue was discovered in JFinal framework v4.9.10 and below. The "set" method of the "Controller" class of jfinal framework is not strictly filtered, which will lead to XSS vulnerabilities in some cases. | 6.1 | More Details |
| CVE-2021-35210 | Contao 4.5.x through 4.9.x before 4.9.16, and 4.10.x through 4.11.x before 4.11.5, allows XSS. It is possible to inject code into the tl_log table that will be executed in the browser when the system log is called in the back end. | 6.1 | More Details |
| CVE-2020-18663 | Cross Site Scripting (XSS) vulnerability in gnuboard5 <=v5.3.2.8 via the act parameter in bbs/move_update.php. | 6.1 | More Details |
| CVE-2020-21783 | In IBOS 4.5.4 the email function has a cross site scripting (XSS) vulnerability in emailbody[content] parameter. | 6.1 | More Details |
| CVE-2020-18661 | Cross Site Scripting (XSS) vulnerability in gnuboard5 <=v5.3.2.8 via the url parameter to bbs/login.php. | 6.1 | More Details |
| CVE-2021-21571 | Dell UEFI BIOS https stack leveraged by the Dell BIOSConnect feature and Dell HTTPS Boot feature contains an improper certificate validation vulnerability. A remote unauthenticated attacker may exploit this vulnerability using a person-in-the-middle attack which may lead to a denial of service and payload tampering. | 5.9 | More Details |
| CVE-2021-32710 | Shopware is an open source eCommerce platform. Potential session hijacking of store customers in versions below 6.3.5.2. We recommend to update to the current version 6.3.5.2. You can get the update to 6.3.5.2 regularly via the Auto-Updater or directly via the download overview. For older versions of 6.1 and 6.2, corresponding security measures are also available via a plugin. For the full range of functions, we recommend updating to the latest Shopware version. | 5.9 | More Details |

| CVE Number | Description | Base Score | Reference |
|---|---|---|---|
| CVE-2020-28097 | The vgacon subsystem in the Linux kernel before 5.8.10 mishandles software scrollback. There is a vgacon_scrolldelta out-of-bounds read, aka CID-973c096f6a85. | 5.9 | More Details |
| CVE-2021-28623 | Adobe Premiere Elements version 5.2 (and earlier) is affected by an insecure temporary file creation vulnerability. An unauthenticated attacker could leverage this vulnerability to call functions against the installer to perform high privileged actions. Exploitation of this issue does not require user interaction. | 5.5 | More Details |
| CVE-2021-26585 | A potential vulnerability has been identified in HPE OneView Global Dashboard release 2.31 which could lead to a local disclosure of privileged information. HPE has provided an update to OneView Global Dashboard. The issue is resolved in 2.32. | 5.5 | More Details |
| CVE-2021-28597 | Adobe Photoshop Elements version 5.2 (and earlier) is affected by an insecure temporary file creation vulnerability. An unauthenticated attacker could leverage this vulnerability to call functions against the installer to perform high privileged actions. Exploitation of this issue does not require user interaction. | 5.5 | More Details |
| CVE-2021-34071 | Heap based buffer overflow in tsMuxer 2.6.16 allows attackers to cause a Denial of Service (DoS) by running the application with a crafted file. | 5.5 | More Details |
| CVE-2021-34070 | Out-of-bounds Read in tsMuxer 2.6.16 allows attackers to cause a Denial of Service (DoS) by running the application with a crafted file. | 5.5 | More Details |
| CVE-2021-34069 | Divide-by-zero bug in tsMuxer 2.6.16 allows attackers to cause a Denial of Service (DoS) by running the application with a crafted file. | 5.5 | More Details |
| CVE-2021-34068 | Heap based buffer overflow in tsMuxer 2.6.16 allows attackers to cause a Denial of Service (DoS) by running the application with a crafted file. | 5.5 | More Details |
| CVE-2021-34067 | Heap based buffer overflow in tsMuxer 2.6.16 allows attackers to cause a Denial of Service (DoS) by running the application with a crafted file. | 5.5 | More Details |
| CVE-2021-20490 | IBM Spectrum Protect Plus 10.1.0 through 10.1.8 could allow a local user to cause a denial of service due to insecure file permission settings. IBM X-Force ID: 197791. | 5.5 | More Details |
| CVE-2021-29775 | IBM Business Automation Workflow 19.0.03 and 20.0 and IBM Cloud Pak for Automation 20.0.3-IF002 and 21.0.1 are vulnerable to cross-site scripting. This vulnerability allows users to embed arbitrary JavaScript code in the Web UI thus altering the intended functionality potentially leading to credentials disclosure within a trusted session. IBM X-Force ID: 203029. | 5.4 | More Details |
| CVE-2020-20391 | Cross Site Scripting vulnerability in GetSimpleCMS 3.4.0a in admin/snippets.php via (1) Add Snippet and (2) Save snippets. | 5.4 | More Details |
| CVE-2020-23710 | Cross Site Scripting (XSS) vulneraiblity in LimeSurvey 4.2.5 on textbox via the Notifications & data feature. | 5.4 | More Details |
| CVE-2021-20477 | IBM Planning Analytics 2.0 is vulnerable to cross-site scripting. This vulnerability allows users to embed arbitrary JavaScript code in the Web UI thus altering the intended functionality potentially leading to credentials disclosure within a trusted session. IBM X-Force ID: 196949. | 5.4 | More Details |
| CVE-2020-18671 | Cross Site Scripting (XSS) vulnerability in Roundcube Mail <=1.4.4 via smtp config in /installer/test.php. | 5.4 | More Details |
| CVE-2021-28584 | Magento versions 2.4.2 (and earlier), 2.4.1-p1 (and earlier) and 2.3.6-p1 (and earlier) are affected by a Path Traversal vulnerability when creating a store with child theme.Successful exploitation could lead to arbitrary file system write by an authenticated attacker. Access to the admin console is required for successful exploitation. | 5.4 | More Details |
| CVE-2021-29676 | IBM Security Verify (IBM Security Verify Privilege Vault 10.9.66) is vulnerable to link injection. By persuading a victim to click on a specially-crafted URL link, a remote attacker could exploit this vulnerability to conduct various attacks against the vulnerable system, including cross-site scripting, cache poisoning or session hijacking | 5.4 | More Details |
| CVE-2020-18668 | Cross Site Scripting (XSS) vulnerabililty in WebPort <=1.19.1 via the description parameter to script/listcalls. | 5.4 | More Details |
| CVE-2021-35501 | PandoraFMS <=7.54 allows Stored XSS by placing a payload in the name field of a visual console. When a user or an administrator visits the console, the XSS payload will be executed. | 5.4 | More Details |

| CVE Number | Description | Base Score | Reference |
|---|---|---|---|
| CVE-2020-26801 | A stored cross-site scripting (XSS) vulnerability was discovered in /Forms/device_vars_1 on TrippLite SU2200RTXL2Ua with firmware version 12.04.0055. This vulnerability allows authenticated attackers to obtain other users' information via a crafted POST request. | 5.4 | More Details |
| CVE-2021-35475 | SAS Environment Manager 2.5 allows XSS through the Name field when creating/editing a server. The XSS will prompt when editing the Configuration Properties. | 5.4 | More Details |
| CVE-2020-18664 | Cross Site Scripting (XSS) vulnerability in WebPort <=1.19.1via the connection name parameter in type-conn. | 5.4 | More Details |
| CVE-2021-20746 | Cross-site scripting vulnerability in WordPress Popular Posts 5.3.2 and earlier allows a remote authenticated attacker to inject an arbitrary script via unspecified vectors. | 5.4 | More Details |
| CVE-2021-20749 | Cross-site scripting vulnerability in Fudousan plugin ver5.7.0 and earlier, Fudousan Plugin Pro Single-User Type ver5.7.0 and earlier, and Fudousan Plugin Pro Multi-User Type ver5.7.0 and earlier allows a remote authenticated attacker to inject an arbitrary script via unspecified vectors. | 5.4 | More Details |
| CVE-2021-29677 | IBM Security Verify (IBM Security Verify Privilege Vault 10.9.66) 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. | 5.4 | More Details |
| CVE-2020-18670 | Cross Site Scripting (XSS) vulneraibility in Roundcube mail .4.4 via database host and user in /installer/test.php. | 5.4 | More Details |
| CVE-2021-29086 | Exposure of sensitive information to an unauthorized actor vulnerability in webapi component in Synology DiskStation Manager (DSM) before 6.2.3-25426-3 allows remote attackers to obtain sensitive information via unspecified vectors. | 5.3 | More Details |
| CVE-2021-32496 | SICK Visionary-S CX up version 5.21.2.29154R are vulnerable to an Inadequate Encryption Strength vulnerability concerning the internal SSH interface solely used by SICK for recovering returned devices. The use of weak ciphers make it easier for an attacker to break the security that protects information transmitted from the client to the SSH server, assuming the attacker has access to the network on which the device is connected. This can increase the risk that encryption will be compromised, leading to the exposure of sensitive user information and man-in-the-middle attacks. | 5.3 | More Details |
| CVE-2021-21003 | In Phoenix Contact FL SWITCH SMCS series products in multiple versions fragmented TCP-Packets may cause a Denial of Service of Web-, SNMP- and ICMP-Echo services. The switching functionality of the device is not affected. | 5.3 | More Details |
| CVE-2021-29965 | A malicious website that causes an HTTP Authentication dialog to be spawned could trick the built-in password manager to suggest passwords for the currently active website instead of the website that triggered the dialog. *This bug only affects Firefox for Android. Other operating systems are unaffected.*. This vulnerability affects Firefox < 89. | 5.3 | More Details |
| CVE-2021-28585 | Magento versions 2.4.2 (and earlier), 2.4.1-p1 (and earlier) and 2.3.6-p1 (and earlier) are affected by an Improper input validation vulnerability in the New customer WebAPI.Successful exploitation could allow an attacker to send unsolicited spam e-mails. | 5.3 | More Details |
| CVE-2021-29955 | A transient execution vulnerability, named Floating Point Value Injection (FPVI) allowed an attacker to leak arbitrary memory addresses and may have also enabled JIT type confusion attacks. (A related vulnerability, Speculative Code Store Bypass (SCSB), did not affect Firefox.). This vulnerability affects Firefox ESR < 78.9 and Firefox < 87. | 5.3 | More Details |
| CVE-2021-27659 | exacqVision Web Service 21.03 does not sufficiently validate, filter, escape, and/or encode user-controllable input before it is placed in output that is used as a web page that is served to other users. | 5.3 | More Details |
| CVE-2021-31615 | Unencrypted Bluetooth Low Energy baseband links in Bluetooth Core Specifications 4.0 through 5.2 may permit an adjacent device to inject a crafted packet during the receive window of the listening device before the transmitting device initiates its packet transmission to achieve full MITM status without terminating the link. When applied against devices establishing or using encrypted links, crafted packets may be used to terminate an existing link, but will not compromise the confidentiality or integrity of the link. | 5.3 | More Details |
| CVE-2021-35302 | Incorrect Access Control for linked Tickets in Zammad 1.0.x up to 4.0.0 allows remote attackers to obtain sensitive information. | 5.3 | More Details |
| CVE-2021-35301 | Incorrect Access Control in Zammad 1.0.x up to 4.0.0 allows remote attackers to obtain sensitive information via the Ticket Article detail view. | 5.3 | More Details |
| CVE-2021-25656 | Stored XSS injection vulnerabilities were discovered in the Avaya Aura Experience Portal Web management which could allow an authenticated user to potentially disclose sensitive information. Affected versions include 7.0 through 7.2.3 (without hotfix) and 8.0.0 (without hotfix). | 5.3 | More Details |

| CVE Number | Description | Base Score | Reference |
|---|---|---|---|
| CVE-2021-32720 | Sylius is an Open Source eCommerce platform on top of Symfony. In versions of Sylius prior to 1.9.5 and 1.10.0-RC.1, part of the details (order ID, order number, items total, and token value) of all placed orders were exposed to unauthorized users. If exploited properly, a few additional information like the number of items in the cart and the date of the shipping may be fetched as well. This data seems to not be crucial nor is personal data, however, could be used for sociotechnical attacks or may expose a few details about shop condition to the third parties. The data possible to aggregate are the number of processed orders or their value in the moment of time. The problem has been patched at Sylius 1.9.5 and 1.10.0-RC.1. There are a few workarounds for the vulnerability. The first possible solution is to hide the problematic endpoints behind the firewall from not logged in users. This would put only the order list under the firewall and allow only authorized users to access it. Once a user is authorized, it will have access to theirs orders only. The second possible solution is to decorate the `\Sylius\Bundle\ApiBundle\Doctrine\QueryCollectionExtension\OrdersByLoggedInUserExtension` and throw `Symfony\Component\Security\Core\Exception\AccessDeniedException` if the class is executed for unauthorized user. | 5.3 | More Details |
| CVE-2021-22338 | There is an XXE injection vulnerability in eCNS280 V100R005C00 and V100R005C10. A module does not perform the strict operation to the input XML message. Attacker can send specific message to exploit this vulnerability, leading to the module denial of service. | 5.3 | More Details |
| CVE-2021-32712 | Shopware is an open source eCommerce platform. Versions prior to 5.6.10 are vulnerable to system information leakage in error handling. Users are recommend to update to version 5.6.10. You can get the update to 5.6.10 regularly via the Auto-Updater or directly via the download overview. | 5.3 | More Details |
| CVE-2021-35525 | PostSRSd before 1.11 allows a denial of service (subprocess hang) if Postfix sends certain long data fields such as multiple concatenated email addresses. NOTE: the PostSRSd maintainer acknowledges "theoretically, this error should never occur ... I'm not sure if there's a reliable way to trigger this condition by an external attacker, but it is a security bug in PostSRSd nevertheless." | 5.3 | More Details |
| CVE-2021-31412 | Improper sanitization of path in default RouteNotFoundError view in com.vaadin:flow-server versions 1.0.0 through 1.0.14 (Vaadin 10.0.0 through 10.0.18), 1.1.0 prior to 2.0.0 (Vaadin 11 prior to 14), 2.0.0 through 2.6.1 (Vaadin 14.0.0 through 14.6.1), and 3.0.0 through 6.0.9 (Vaadin 15.0.0 through 19.0.8) allows network attacker to enumerate all available routes via crafted HTTP request when application is running in production mode and no custom handler for NotFoundException is provided. | 5.3 | More Details |
| CVE-2020-18665 | Directory Traversal vulnerability in WebPort <=1.19.1 in tags of system settings. | 5.3 | More Details |
| CVE-2021-22329 | There has a license management vulnerability in some Huawei products. An attacker with high privilege needs to perform specific operations to exploit the vulnerability on the affected device. Due to improper license management of the device, as a result, the license file can be applied and affect integrity of the device. Affected product versions include:S12700 V200R007C01,V200R007C01B102,V200R008C00,V200R010C00SPC300,V200R011C00,V200R011C00SPC100,V200R011C10;S1700 V200R010C00SPC300,V200R011C00,V200R011C00SPC100,V200R011C10;S2700 V200R008C00,V200R010C00SPC300,V200R011C00,V200R011C00SPC100,V200R011C10;S5700 V200R008C00,V200R010C00SPC300,V200R011C00,V200R011C00SPC100,V200R011C10,V200R011C10SPC100;S6700 V200R008C00,V200R010C00SPC300,V200R011C00,V200R011C00SPC100,V200R011C10,V200R011C10SPC100;S7700 V200R008C00,V200R010C00SPC300,V200R011C00,V200R011C00SPC100,V200R011C10;S9700 V200R007C01,V200R007C01B102,V200R008C00,V200R010C00SPC300,V200R011C00,V200R011C00SPC100,V200R011C10. | 4.9 | More Details |
| CVE-2021-20583 | IBM Security Verify (IBM Security Verify Privilege Vault 10.9.66) could disclose sensitive information through an HTTP GET request by a privileged user due to improper input validation.. IBM X-Force ID: 199396. | 4.9 | More Details |
| CVE-2021-32709 | Shopware is an open source eCommerce platform. Creation of order credits was not validated by ACL in admin orders. Users are recommend to update to the current version 6.4.1.1. You can get the update to 6.4.1.1 regularly via the Auto-Updater or directly via the download overview. For older versions of 6.1, 6.2, and 6.3, corresponding security measures are also available via a plugin. For the full range of functions, we recommend updating to the latest Shopware version. | 4.9 | More Details |
| CVE-2021-22341 | There is a memory leak vulnerability in Huawei products. A resource management weakness exists in a module. Attackers with high privilege can exploit this vulnerability by performing some operations. This can lead to memory leak. Affected product versions include:IPS Module V500R005C00SPC100,V500R005C00SPC200;NGFW Module V500R005C00SPC100,V500R005C00SPC200;NIP6300 V500R005C00SPC100,V500R005C10SPC200;NIP6600 V500R005C00SPC100,V500R005C00SPC200;Secospace USG6300 V500R005C00SPC100,V500R005C00SPC200;Secospace USG6500 V500R005C00SPC100,V500R005C10SPC200;Secospace USG6600 V500R005C00SPC100,V500R005C00SPC200. | 4.9 | More Details |
| CVE-2021-25649 | An information disclosure vulnerability was discovered in the directory and file management of Avaya Aura Utility Services. This vulnerability may potentially allow any local user to access system functionality and configuration information that should only be available to a privileged user. Affects all 7.x versions of Avaya Aura Utility Services | 4.9 | More Details |
| CVE-2021-25652 | An information disclosure vulnerability was discovered in the directory and file management of Avaya Aura Appliance Virtualization Platform Utilities (AVPU). This vulnerability may potentially allow any local user to access system functionality and configuration information that should only be available to a privileged user. Affects versions 8.0.0.0 through 8.1.3.1 of AVPU. | 4.9 | More Details |
| CVE-2021-28977 | Cross Site Scripting vulnerability in GetSimpleCMS 3.3.16 in admin/upload.php by adding comments or jpg and other file header information to the content of xla, pages, and gzip files, | 4.8 | More Details |
| CVE-2020-20389 | Cross Site Scripting (XSS) vulnerability in GetSimpleCMS 3.4.0a in admin/edit.php. | 4.8 | More Details |

| CVE Number | Description | Base Score | Reference |
|---|---|---|---|
| CVE-2021-33515 | The submission service in Dovecot before 2.3.15 allows STARTTLS command injection in lib-smtp. Sensitive information can be redirected to an attacker-controlled address. | 4.8 | More Details |
| CVE-2021-32713 | Shopware is an open source eCommerce platform. Versions prior to 5.6.10 suffer from an authenticated stored XSS in administration vulnerability. Users are recommend to update to the version 5.6.10. You can get the update to 5.6.10 regularly via the Auto-Updater or directly via the download overview. | 4.8 | More Details |
| CVE-2021-32721 | PowerMux is a drop-in replacement for Go's http.ServeMux. In PowerMux versions prior to 1.1.1, attackers may be able to craft phishing links and other open redirects by exploiting the trailing slash redirection feature. This may lead to users being redirected to untrusted sites after following an attacker crafted link. The issue is resolved in v1.1.1. There are no existing workarounds. | 4.7 | More Details |
| CVE-2020-4885 | IBM Db2 for Linux, UNIX and Windows (includes Db2 Connect Server) 11.5 could allow a local user to access and change the configuration of Db2 due to a race condition of a symbolic link,. IBM X-Force ID: 190909. | 4.7 | More Details |
| CVE-2021-33624 | In kernel/bpf/verifier.c in the Linux kernel before 5.12.13, a branch can be mispredicted (e.g., because of type confusion) and consequently an unprivileged BPF program can read arbitrary memory locations via a side-channel attack, aka CID-9183671af6db. | 4.7 | More Details |
| CVE-2021-25655 | A vulnerability in the system Service Menu component of Avaya Aura Experience Portal may allow URL Redirection to any untrusted site through a crafted attack. Affected versions include 7.0 through 7.2.3 (without hotfix) and 8.0.0 (without hotfix). | 4.4 | More Details |
| CVE-2021-32716 | Shopware is an open source eCommerce platform. In versions prior to 6.4.1.1 the admin api has exposed some internal hidden fields when an association has been loaded with a to many reference. Users are recommend to update to version 6.4.1.1. You can get the update to 6.4.1.1 regularly via the Auto-Updater or directly via the download overview. For older versions of 6.1, 6.2, and 6.3, corresponding security measures are also available via a plugin. | 4.4 | More Details |
| CVE-2021-29480 | Ratpack is a toolkit for creating web applications. In versions prior to 1.9.0, the client side session module uses the application startup time as the signing key by default. This means that if an attacker can determine this time, and if encryption is not also used (which is recommended, but is not on by default), the session data could be tampered with by someone with the ability to write cookies. The default configuration is unsuitable for production use as an application restart renders all sessions invalid and is not multi-host compatible, but its use is not actively prevented. As of Ratpack 1.9.0, the default value is a securely randomly generated value, generated at application startup time. As a workaround, supply an alternative signing key, as per the documentation's recommendation. | 4.4 | More Details |
| CVE-2021-29693 | IBM AIX 7.1, 7.2, and VIOS 3.1 could allow a local user that is in the with elevated group privileges to cause a denial of service due to a vulnerability in the lpd daemon. IBM X-Force ID: 200255. | 4.4 | More Details |
| CVE-2021-20580 | IBM Planning Analytics 2.0 could be vulnerable to cross-site request forgery (CSRF) which could allow an attacker to execute malicious and unauthorized actions transmitted from a user that the website trusts. IBM X-Force ID: 198241. | 4.3 | More Details |
| CVE-2020-21788 | In CRMEB 3.1.0+ strict domain name filtering leads to SSRF(Server-Side Request Forgery). The vulnerable code is in file /crmeb/app/admin/controller/store/CopyTaobao.php. | 4.3 | More Details |
| CVE-2021-29963 | Address bar search suggestions in private browsing mode were re-using session data from normal mode. *This bug only affects Firefox for Android. Other operating systems are unaffected.*. This vulnerability affects Firefox < 89. | 4.3 | More Details |
| CVE-2021-28579 | Adobe Connect version 11.2.1 (and earlier) is affected by an Improper access control vulnerability that can lead to the elevation of privileges. An attacker with 'Learner' permissions can leverage this scenario to access the list of event participants. | 4.3 | More Details |
| CVE-2021-29962 | Firefox for Android would become unstable and hard-to-recover when a website opened too many popups. *This bug only affects Firefox for Android. Other operating systems are unaffected.*. This vulnerability affects Firefox < 89. | 4.3 | More Details |
| CVE-2021-29961 | When styling and rendering an oversized `<select>` element, Firefox did not apply correct clipping which allowed an attacker to paint over the user interface. This vulnerability affects Firefox < 89. | 4.3 | More Details |
| CVE-2021-20413 | IBM Guardium Data Encryption (GDE) 4.0.0.4 could allow a remote attacker to obtain sensitive information when a detailed technical error message is returned in the browser. This information could be used in further attacks against the system. IBM X-Force ID: 196212. | 4.3 | More Details |
| CVE-2021-28576 | Adobe Animate version 21.0.5 (and earlier) is affected by an Out-of-bounds Read vulnerability when parsing a specially crafted file. An unauthenticated attacker could leverage this vulnerability to disclose sensitive information in the context of the current user. Exploitation of this issue requires user interaction in that a victim must open a malicious file. | 4.3 | More Details |

| CVE Number | Description | Base Score | Reference |
|---|---|---|---|
| CVE-2021-28575 | Adobe Animate version 21.0.5 (and earlier) is affected by an Out-of-bounds Read vulnerability when parsing a specially crafted file. An unauthenticated attacker could leverage this vulnerability to disclose sensitive information in the context of the current user. Exploitation of this issue requires user interaction in that a victim must open a malicious file. | 4.3 | More Details |
| CVE-2021-28574 | Adobe Animate version 21.0.5 (and earlier) is affected by an Out-of-bounds Read vulnerability when parsing a specially crafted file. An unauthenticated attacker could leverage this vulnerability to disclose sensitive information in the context of the current user. Exploitation of this issue requires user interaction in that a victim must open a malicious file. | 4.3 | More Details |
| CVE-2021-29751 | IBM Business Automation Workflow 18.0, 19.0, and 20.0 and IBM Business Process Manager 8.5 and 8.6 could allow an authenticated user to obtain sensitive information about another user under nondefault configurations. IBM X-Force ID: 201779. | 4.3 | More Details |
| CVE-2021-28573 | Adobe Animate version 21.0.5 (and earlier) is affected by an Out-of-bounds Read vulnerability when parsing a specially crafted file. An unauthenticated attacker could leverage this vulnerability to disclose sensitive information in the context of the current user. Exploitation of this issue requires user interaction in that a victim must open a malicious file. | 4.3 | More Details |
| CVE-2021-23992 | Thunderbird did not check if the user ID associated with an OpenPGP key has a valid self signature. An attacker may create a crafted version of an OpenPGP key, by either replacing the original user ID, or by adding another user ID. If Thunderbird imports and accepts the crafted key, the Thunderbird user may falsely conclude that the false user ID belongs to the correspondent. This vulnerability affects Thunderbird < 78.9.1. | 4.3 | More Details |
| CVE-2020-28200 | The Sieve engine in Dovecot before 2.3.15 allows Uncontrolled Resource Consumption, as demonstrated by a situation with a complex regular expression for the regex extension. | 4.3 | More Details |
| CVE-2021-35300 | Text injection/Content Spoofing in 404 page in Zammad 1.0.x up to 4.0.0 could allow remote attackers to manipulate users into visiting the attackers' page. | 4.3 | More Details |
| CVE-2021-24001 | A compromised content process could have performed session history manipulations it should not have been able to due to testing infrastructure that was not restricted to testing-only configurations. This vulnerability affects Firefox < 88. | 4.3 | More Details |
| CVE-2021-27658 | exacqVision Enterprise Manager 20.12 does not sufficiently validate, filter, escape, and/or encode user-controllable input before it is placed in output that is used as a web page that is served to other users. | 4.3 | More Details |
| CVE-2021-29960 | Firefox used to cache the last filename used for printing a file. When generating a filename for printing, Firefox usually suggests the web page title. The caching and suggestion techniques combined may have lead to the title of a website visited during private browsing mode being stored on disk. This vulnerability affects Firefox < 89. | 4.3 | More Details |
| CVE-2021-29959 | When a user has already allowed a website to access microphone and camera, disabling camera sharing would not fully prevent the website from re-enabling it without an additional prompt. This was only possible if the website kept recording with the microphone until re-enabling the camera. This vulnerability affects Firefox < 89. | 4.3 | More Details |
| CVE-2021-29956 | OpenPGP secret keys that were imported using Thunderbird version 78.8.1 up to version 78.10.1 were stored unencrypted on the user's local disk. The master password protection was inactive for those keys. Version 78.10.2 will restore the protection mechanism for newly imported keys, and will automatically protect keys that had been imported using affected Thunderbird versions. This vulnerability affects Thunderbird < 78.10.2. | 4.3 | More Details |
| CVE-2021-29958 | When a download was initiated, the client did not check whether it was in normal or private browsing mode, which led to private mode cookies being shared in normal browsing mode. This vulnerability affects Firefox for iOS < 34. | 4.3 | More Details |
| CVE-2021-29957 | If a MIME encoded email contains an OpenPGP inline signed or encrypted message part, but also contains an additional unprotected part, Thunderbird did not indicate that only parts of the message are protected. This vulnerability affects Thunderbird < 78.10.2. | 4.3 | More Details |
| CVE-2021-22340 | There is a multiple threads race condition vulnerability in Huawei product. A race condition exists for concurrent I/O read by multiple threads. An attacker with the root permission can exploit this vulnerability by performing some operations. Successful exploitation of this vulnerability may cause the system to crash. Affected product versions include: ManageOne 6.5.1.SPC200, 8.0.0,8.0.0-LCND81, 8.0.0.SPC100, 8.0.1,8.0.RC2, 8.0.RC3, 8.0.RC3.SPC100;SMC2.0 V600R019C10SPC700,V600R019C10SPC702, V600R019C10SPC703,V600R019C10SPC800, V600R019C10SPC900, V600R019C10SPC910, V600R019C10SPC920, V600R019C10SPC921, V600R019C10SPC922, V600R019C10SPC930, V600R019C10SPC931 | 4.1 | More Details |
| CVE-2021-32823 | In the bindata RubyGem before version 2.4.10 there is a potential denial-of-service vulnerability. In affected versions it is very slow for certain classes in BinData to be created. For example BinData::Bit100000, BinData::Bit100001, BinData::Bit100002, BinData::Bit<N>. In combination with <user_input>.constantize there is a potential for a CPU-based DoS. In version 2.4.10 bindata improved the creation time of Bits and Integers. | 3.7 | More Details |
| CVE-2021-28587 | After Effects versions 18.0 (and earlier) are affected by an out-of-bounds read vulnerability that could lead to disclosure of sensitive memory. An attacker could leverage this vulnerability to bypass mitigations such as ASLR. Exploitation of this issue requires user interaction in that a victim must open a malicious file. | 3.3 | More Details |

| CVE Number | Description | Base Score | Reference |
|---|---|---|---|
| CVE-2021-31506 | This vulnerability allows remote attackers to disclose sensitive information on affected installations of OpenText Brava! Desktop Build 16.6.4.55. User interaction is required to exploit this vulnerability in that the target must visit a malicious page or open a malicious file. The specific flaw exists within the parsing of PDF files. The issue results from the lack of proper validation of user-supplied data, which can result in a read past the end of an allocated data structure. An attacker can leverage this in conjunction with other vulnerabilities to execute arbitrary code in the context of the current process. Was ZDI-CAN-13674. | 3.3 | More Details |
| CVE-2021-27040 | A maliciously crafted DWG file can be forced to read beyond allocated boundaries when parsing the DWG file. This vulnerability can be exploited to execute arbitrary code. | 3.3 | More Details |
| CVE-2021-32719 | RabbitMQ is a multi-protocol messaging broker. In rabbitmq-server prior to version 3.8.18, when a federation link was displayed in the RabbitMQ management UI via the `rabbitmq_federation_management` plugin, its consumer tag was rendered without proper <script> tag sanitization. This potentially allows for JavaScript code execution in the context of the page. The user must be signed in and have elevated permissions (manage federation upstreams and policies) for this to occur. The vulnerability is patched in RabbitMQ 3.8.18. As a workaround, disable the `rabbitmq_federation_management` plugin and use [CLI tools](https://www.rabbitmq.com/cli.html) instead. | 3.1 | More Details |
| CVE-2021-32718 | RabbitMQ is a multi-protocol messaging broker. In rabbitmq-server prior to version 3.8.17, a new user being added via management UI could lead to the user's bane being rendered in a confirmation message without proper `<script>` tag sanitization, potentially allowing for JavaScript code execution in the context of the page. In order for this to occur, the user must be signed in and have elevated permissions (other user management). The vulnerability is patched in RabbitMQ 3.8.17. As a workaround, disable `rabbitmq_management` plugin and use CLI tools for management operations and Prometheus and Grafana for metrics and monitoring. | 3.1 | More Details |
| CVE-2021-24000 | A race condition with requestPointerLock() and setTimeout() could have resulted in a user interacting with one tab when they believed they were on a separate tab. In conjunction with certain elements (such as <input type="file">) this could have led to an attack where a user was confused about the origin of the webpage and potentially disclosed information they did not intend to. This vulnerability affects Firefox < 88. | 3.1 | More Details |
| CVE-2021-33604 | URL encoding error in development mode handler in com.vaadin:flow-server versions 2.0.0 through 2.6.1 (Vaadin 14.0.0 through 14.6.1), 3.0.0 through 6.0.9 (Vaadin 15.0.0 through 19.0.8) allows local user to execute arbitrary JavaScript code by opening crafted URL in browser. | 2.5 | More Details |
| CVE-2021-29948 | Signatures are written to disk before and read during verification, which might be subject to a race condition when a malicious local process or user is replacing the file. This vulnerability affects Thunderbird < 78.10. | 2.5 | More Details |
| CVE-2020-18666 | Rejected reason: DO NOT USE THIS CANDIDATE NUMBER. ConsultIDs: CVE-2020-18664. Reason: This candidate is a duplicate of CVE-2020-18664. Notes: All CVE users should reference CVE-2020-18664 instead of this candidate. All references and descriptions in this candidate have been removed to prevent accidental usage | N/A | More Details |
| CVE-2011-1942 | Rejected reason: DO NOT USE THIS CANDIDATE NUMBER. ConsultIDs: none. Reason: This candidate was withdrawn by its CNA. Notes: none | N/A | More Details |
| CVE-2021-25950 | Rejected reason: DO NOT USE THIS CANDIDATE NUMBER. ConsultIDs: none. Reason: This candidate was withdrawn by its CNA. Further investigation showed that it was not a security issue. Notes: none | N/A | More Details |
| CVE-2021-3526 | Rejected reason: DO NOT USE THIS CANDIDATE NUMBER. ConsultIDs: none. Reason: This candidate was withdrawn by its CNA. Notes: none | N/A | More Details |
| CVE-2018-1138 | Rejected reason: DO NOT USE THIS CANDIDATE NUMBER. ConsultIDs: none. Reason: This candidate was withdrawn by its CNA. Notes: Assigned as a duplicate of CVE-2019-14827 | N/A | More Details |
| CVE-2021-34183 | Rejected reason: DO NOT USE THIS CANDIDATE NUMBER. ConsultIDs: none. Reason: This candidate was withdrawn by its CNA. Further investigation showed that it was not a security issue. Notes: none | N/A | More Details |
| CVE-2011-2926 | Rejected reason: DO NOT USE THIS CANDIDATE NUMBER. ConsultIDs: none. Reason: This candidate was withdrawn by its CNA. Notes: none | N/A | More Details |
| CVE-2011-0023 | Rejected reason: DO NOT USE THIS CANDIDATE NUMBER. ConsultIDs: none. Reason: This candidate was withdrawn by its CNA. Notes: none | N/A | More Details |
| CVE-2011-1177 | Rejected reason: DO NOT USE THIS CANDIDATE NUMBER. ConsultIDs: none. Reason: This candidate was withdrawn by its CNA. Notes: none | N/A | More Details |
| CVE-2021-3556 | Rejected reason: DO NOT USE THIS CANDIDATE NUMBER. ConsultIDs: none. Reason: This candidate was withdrawn by its CNA. Notes: Assigned but a duplicate for CVE-2021-3559 | N/A | More Details |

| CVE Number | Description | Base Score | Reference |
| --- | --- | --- | --- |
| CVE-2011-1955 | Rejected reason: DO NOT USE THIS CANDIDATE NUMBER. ConsultIDs: none. Reason: This candidate was withdrawn by its CNA. Notes: none | N/A | More Details |