SingCERT
Singapore Cyber Emergency Response Team

Security Bulletin 21 April 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-2021-24028	An invalid free in Thrift's table-based serialization can cause the application to crash or potentially result in code execution or other undesirable effects. This issue affects Facebook Thrift prior to v2021.02.22.00.	9.8	More Details
CVE-2020-27238	An exploitable SQL injection vulnerability exists in 'getAssets.jsp' page of OpenClinic GA 5.173.3. The code parameter in the getAssets.jsp page is vulnerable to unauthenticated SQL injection. An attacker can make an authenticated HTTP request to trigger this vulnerability.	9.8	More Details
CVE-2021-31162	In the standard library in Rust before 1.52.0, a double free can occur in the Vec::from_iter function if freeing the element panics.	9.8	More Details
CVE-2021-27112	LightCMS v1.3.5 contains a remote code execution vulnerability in /app/Http/Controllers/Admin/NEditorController.php during the downloading of external images.	9.8	More Details

CVE Number	Description	Base Score	Reference
CVE-2021-27691	Command Injection in Tenda G0 routers with firmware versions v15.11.0.6(9039)_CN and v15.11.0.5(5876)_CN , and Tenda G1 and G3 routers with firmware versions v15.11.0.17(9502)_CN or v15.11.0.16(9024)_CN allows remote attackers to execute arbitrary OS commands via a crafted action/setDebugCfg request. This occurs because the "formSetDebugCfg" function executes glibc's system function with untrusted input.	9.8	More Details
CVE-2021-27692	Command Injection in Tenda G1 and G3 routers with firmware versions v15.11.0.17(9502)_CN or v15.11.0.16(9024)_CN allows remote attackers to execute arbitrary OS commands via a crafted "action/umountUSBPartition" request. This occurs because the "formSetUSBPartitionUmount" function executes the "doSystemCmd" function with untrusted input.	9.8	More Details
CVE-2021-31414	The unofficial vscode-rpm-spec extension before 0.3.2 for Visual Studio Code allows remote code execution via a crafted workspace configuration.	9.8	More Details
CVE-2020-2509	A command injection vulnerability has been reported to affect QTS and QuTS hero. If exploited, this vulnerability allows attackers to execute arbitrary commands in a compromised application. We have already fixed this vulnerability in the following versions: QTS 4.5.2.1566 Build 20210202 and later QTS 4.5.1.1495 Build 20201123 and later QTS 4.3.6.1620 Build 20210322 and later QTS 4.3.4.1632 Build 20210324 and later QTS 4.3.3.1624 Build 20210416 and later QTS 4.2.6 Build 20210327 and later QuTS hero h4.5.1.1491 build 20201119 and later	9.8	More Details
CVE-2020-36195	An SQL injection vulnerability has been reported to affect QNAP NAS running Multimedia Console or the Media Streaming add-on. If exploited, the vulnerability allows remote attackers to obtain application information. QNAP has already fixed this vulnerability in the following versions of Multimedia Console and the Media Streaming add-on. QTS 4.3.3: Media Streaming add-on 430.1.8.10 and later QTS 4.3.6: Media Streaming add-on 430.1.8.8 and later QTS 4.4.x and later: Multimedia Console 1.3.4 and later We have also fixed this vulnerability in the following versions of QTS 4.3.3 and QTS 4.3.6, respectively: QTS 4.3.3.1624 Build 20210416 or later QTS 4.3.6.1620 Build 20210322 or later	9.8	More Details
CVE-2021-23376	This affects all versions of package ffmpegdotjs. If attacker-controlled user input is given to the trimvideo 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.	9.8	More Details

CVE Number	Description	Base Score	Reference
CVE-2021-23377	This affects all versions of package onion-oled-js. If attacker-controlled user input is given to the scroll 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.	9.8	More Details
CVE-2021-23378	This affects all versions of package picotts. If attacker-controlled user input is given to the say 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.	9.8	More Details
CVE-2021-20991	In Fibaro Home Center 2 and Lite devices with firmware version 4.540 and older an authenticated user can run commands as root user using a command injection vulnerability.	9.8	More Details
CVE-2020-27240	An exploitable SQL injection vulnerability exists in ‘getAssets.jsp’ page of OpenClinic GA 5.173.3. The componentStatus parameter in the getAssets.jsp page is vulnerable to unauthenticated SQL injection An attacker can make an authenticated HTTP request to trigger this vulnerability.	9.8	More Details
CVE-2020-27241	An exploitable SQL injection vulnerability exists in ‘getAssets.jsp’ page of OpenClinic GA 5.173.3. The serialnumber parameter in the getAssets.jsp page is vulnerable to unauthenticated SQL injection. An attacker can make an authenticated HTTP request to trigger this vulnerability.	9.8	More Details
CVE-2021-28793	vscode-restructuredtext before 146.0.0 contains an incorrect access control vulnerability, where a crafted project folder could execute arbitrary binaries via crafted workspace configuration.	9.8	More Details
CVE-2020-35313	A server-side request forgery (SSRF) vulnerability in the addCustomThemePluginRepository function in index.php in WonderCMS 3.1.3 allows remote attackers to execute arbitrary code via a crafted URL to the theme/plugin installer.	9.8	More Details
CVE-2020-27239	An exploitable SQL injection vulnerability exists in ‘getAssets.jsp’ page of OpenClinic GA 5.173.3. The assetStatus parameter in the getAssets.jsp page is vulnerable to unauthenticated SQL injection An attacker can make an authenticated HTTP request to trigger this vulnerability.	9.8	More Details
CVE-2020-28592	A heap-based buffer overflow vulnerability exists in the configuration server functionality of the Cosori Smart 5.8-Quart Air Fryer CS158-AF 1.1.0. A specially crafted JSON object can lead to remote code execution. An attacker can send a malicious packet to trigger this vulnerability.	9.8	More Details

CVE Number	Description	Base Score	Reference
CVE-2020-27237	An exploitable SQL injection vulnerability exists in ‘getAssets.jsp’ page of OpenClinic GA 5.173.3. The code parameter in the The nomenclature parameter in the getAssets.jsp page is vulnerable to unauthenticated SQL injection. An attacker can make an authenticated HTTP request to trigger this vulnerability.	9.8	More Details
CVE-2021-27850	A critical unauthenticated remote code execution vulnerability was found all recent versions of Apache Tapestry. The affected versions include 5.4.5, 5.5.0, 5.6.2 and 5.7.0. The vulnerability I have found is a bypass of the fix for CVE-2019-0195. Recap: Before the fix of CVE-2019-0195 it was possible to download arbitrary class files from the classpath by providing a crafted asset file URL. An attacker was able to download the file `AppModule.class` by requesting the URL `http://localhost:8080/assets/something/services/AppModule.class` which contains a HMAC secret key. The fix for that bug was a blacklist filter that checks if the URL ends with `.class`, `.properties` or `.xml`. Bypass: Unfortunately, the blacklist solution can simply be bypassed by appending a `/` at the end of the URL: `http://localhost:8080/assets/something/services/AppModule.class/` The slash is stripped after the blacklist check and the file `AppModule.class` is loaded into the response. This class usually contains the HMAC secret key which is used to sign serialized Java objects. With the knowledge of that key an attacker can sign a Java gadget chain that leads to RCE (e.g. CommonsBeanUtils1 from ysoserial). Solution for this vulnerability: * For Apache Tapestry 5.4.0 to 5.6.1, upgrade to 5.6.2 or later. * For Apache Tapestry 5.7.0, upgrade to 5.7.1 or later.	9.8	More Details
CVE-2021-28797	A stack-based buffer overflow vulnerability has been reported to affect QNAP NAS devices running Surveillance Station. If exploited, this vulnerability allows attackers to execute arbitrary code. QNAP have already fixed this vulnerability in the following versions: Surveillance Station 5.1.5.4.3 (and later) for ARM CPU NAS (64bit OS) and x86 CPU NAS (64bit OS) Surveillance Station 5.1.5.3.3 (and later) for ARM CPU NAS (32bit OS) and x86 CPU NAS (32bit OS)	9.8	More Details
CVE-2020-19778	Incorrect Access Control in Shopxo v1.4.0 and v1.5.0 allows remote attackers to gain privileges in "/index.php" by manipulating the parameter "user_id" in the HTML request.	9.8	More Details
CVE-2021-27113	An issue was discovered in D-Link DIR-816 A2 1.10 B05 devices. An HTTP request parameter is used in command string construction within the handler function of the /goform/addRouting route. This could lead to Command Injection via Shell Metacharacters.	9.8	More Details

CVE Number	Description	Base Score	Reference
CVE-2021-27114	An issue was discovered in D-Link DIR-816 A2 1.10 B05 devices. Within the handler function of the /goform/addassignment route, a very long text entry for the"'s_ip" and "s_mac" fields could lead to a Stack-Based Buffer Overflow and overwrite the return address.	9.8	More Details
CVE-2021-28300	NULL Pointer Dereference in the "isomedia/track.c" module's "MergeTrack()" function of GPAC v0.5.2 allows attackers to execute arbitrary code or cause a Denial-of-Service (DoS) by uploading a malicious MP4 file.	9.8	More Details
CVE-2020-29592	An issue was discovered in Orchard before 1.10. A broken access control issue in Orchard components that use the TinyMCE HTML editor's file upload allows an attacker to upload dangerous executables that bypass the file types allowed (regardless of the file types allowed list in Media settings).	9.8	More Details
CVE-2021-27130	Online Reviewer System 1.0 contains a SQL injection vulnerability through authentication bypass, which may lead to a reverse shell upload.	9.8	More Details
CVE-2021-27705	Buffer Overflow in Tenda G1 and G3 routers with firmware v15.11.0.17(9502)_CN allows remote attackers to execute arbitrary code via a crafted action/"qosIndex "request. This occurs because the "formQOSRuleDel" function directly passes the parameter "qosIndex" to strcpy without limit.	9.8	More Details
CVE-2021-27706	Buffer Overflow in Tenda G1 and G3 routers with firmware version V15.11.0.17(9502)_CN allows remote attackers to execute arbitrary code via a crafted action/"IPMacBindIndex "request. This occurs because the "formIPMacBindDel" function directly passes the parameter "IPMacBindIndex" to strcpy without limit.	9.8	More Details
CVE-2021-27707	Buffer Overflow in Tenda G1 and G3 routers with firmware v15.11.0.17(9502)_CN allows remote attackers to execute arbitrary code via a crafted action/"portMappingIndex "request. This occurs because the "formDelPortMapping" function directly passes the parameter "portMappingIndex" to strcpy without limit.	9.8	More Details
CVE-2021-27258	This vulnerability allows remote attackers to execute escalate privileges on affected installations of SolarWinds Orion Platform 2020.2. Authentication is not required to exploit this vulnerability. The specific flaw exists within the SaveUserSetting endpoint. The issue results from improper restriction of this endpoint to unprivileged users. An attacker can leverage this vulnerability to escalate privileges their privileges from Guest to Administrator. Was ZDI-CAN-11903.	9.8	More Details

CVE Number	Description	Base Score	Reference
CVE-2021-27708	Command Injection in TOTOLINK X5000R router with firmware v9.1.0u.6118_B20201102, and TOTOLINK A720R router with firmware v4.1.5cu.470_B20200911 allows remote attackers to execute arbitrary OS commands by sending a modified HTTP request. This occurs because the function executes glibc's system function with untrusted input. In the function, "command" parameter is directly passed to the attacker, allowing them to control the "command" field to attack the OS.	9.8	More Details
CVE-2021-27710	Command Injection in TOTOLINK X5000R router with firmware v9.1.0u.6118_B20201102, and TOTOLINK A720R router with firmware v4.1.5cu.470_B20200911 allows remote attackers to execute arbitrary OS commands by sending a modified HTTP request. This occurs because the function executes glibc's system function with untrusted input. In the function, "ip" parameter is directly passed to the attacker, allowing them to control the "ip" field to attack the OS.	9.8	More Details
CVE-2021-30459	A SQL Injection issue in the SQL Panel in Jazzband Django Debug Toolbar before 1.11.1, 2.x before 2.2.1, and 3.x before 3.2.1 allows attackers to execute SQL statements by changing the raw_sql input field of the SQL explain, analyze, or select form.	9.8	More Details
CVE-2020-35314	A remote code execution vulnerability in the installUpdateThemePluginAction function in index.php in WonderCMS 3.1.3, allows remote attackers to upload a custom plugin which can contain arbitrary code and obtain a webshell via the theme/plugin installer.	9.8	More Details

CVE Number	Description	Base Score	Reference
CVE-2021-28827	The Administration GUI component of TIBCO Software Inc.'s TIBCO Administrator - Enterprise Edition, TIBCO Administrator - Enterprise Edition, TIBCO Administrator - Enterprise Edition Distribution for TIBCO Silver Fabric, TIBCO Administrator - Enterprise Edition Distribution for TIBCO Silver Fabric, TIBCO Administrator - Enterprise Edition for z/Linux, TIBCO Administrator - Enterprise Edition for z/Linux, TIBCO Runtime Agent, TIBCO Runtime Agent, TIBCO Runtime Agent for z/Linux, and TIBCO Runtime Agent for z/Linux contains an easily exploitable vulnerability that allows an unauthenticated attacker to social engineer a legitimate user with network access to execute a Stored XSS attack targeting the affected system. A successful attack using this vulnerability requires human interaction from a person other than the attacker. Affected releases are TIBCO Software Inc.'s TIBCO Administrator - Enterprise Edition: versions 5.10.2 and below, TIBCO Administrator - Enterprise Edition: versions 5.11.0 and 5.11.1, TIBCO Administrator - Enterprise Edition Distribution for TIBCO Silver Fabric: versions 5.10.2 and below, TIBCO Administrator - Enterprise Edition Distribution for TIBCO Silver Fabric: versions 5.11.0 and 5.11.1, TIBCO Administrator - Enterprise Edition for z/Linux: versions 5.10.2 and below, TIBCO Administrator - Enterprise Edition for z/Linux: versions 5.11.0 and 5.11.1, TIBCO Runtime Agent: versions 5.10.2 and below, TIBCO Runtime Agent: versions 5.11.0 and 5.11.1, TIBCO Runtime Agent for z/Linux: versions 5.10.2 and below, and TIBCO Runtime Agent for z/Linux: versions 5.11.0 and 5.11.1.	9.6	More Details
CVE-2021-29459	XWiki Platform is a generic wiki platform offering runtime services for applications built on top of it. It is possible to persistently inject scripts in XWiki versions prior to 12.6.3 and 12.8. Unregistred users can fill simple text fields. Registered users can fill in their personal information and (if they have edit rights) fill the values of static lists using App Within Minutes. There is no easy workaround except upgrading XWiki. The vulnerability has been patched on XWiki 12.8 and 12.6.3.	9.6	More Details
CVE-2021-29451	Portofino is an open source web development framework. Portofino before version 5.2.1 did not properly verify the signature of JSON Web Tokens. This allows forging a valid JWT. The issue will be patched in the upcoming 5.2.1 release.	9.1	More Details
CVE-2021-26830	SQL Injection in Tribalsystems Zenario CMS 8.8.52729 allows remote attackers to access the database or delete the plugin. This is accomplished via the `ID` input field of ajax.php in the `Pugin library - delete` module.	9.1	More Details

OTHER VULNERABILITIES

CVE Number	Description	Base Score	Reference
CVE-2021-27181	An issue was discovered in MDaemon before 20.0.4. Remote Administration allows an attacker to perform a fixation of the anti-CSRF token. In order to exploit this issue, the user has to click on a malicious URL provided by the attacker and successfully authenticate into the application. Having the value of the anti-CSRF token, the attacker may trick the user into visiting his malicious page and performing any request with the privileges of attacked user.	8.8	More Details
CVE-2021-3493	The overlayfs implementation in the linux kernel did not properly validate with respect to user namespaces the setting of file capabilities on files in an underlying file system. Due to the combination of unprivileged user namespaces along with a patch carried in the Ubuntu kernel to allow unprivileged overlay mounts, an attacker could use this to gain elevated privileges.	8.8	More Details
CVE-2021-27248	This vulnerability allows network-adjacent attackers to execute arbitrary code on affected installations of D-Link DAP-2020 v1.01rc001 Wi-Fi access points. Authentication is not required to exploit this vulnerability. The specific flaw exists within the processing of CGI scripts. When parsing the getpage parameter, the process does not properly validate the length of user-supplied data prior to copying it to a fixed-length stack-based buffer. An attacker can leverage this vulnerability to execute code in the context of root. Was ZDI-CAN-10932.	8.8	More Details
CVE-2021-27251	This vulnerability allows network-adjacent attackers to execute arbitrary code on affected installations of NETGEAR Nighthawk R7800. Authentication is not required to exploit this vulnerability The specific flaw exists within handling of firmware updates. The issue results from a fallback to a insecure protocol to deliver updates. An attacker can leverage this vulnerability to execute code in the context of root. Was ZDI-CAN-12308.	8.8	More Details
CVE-2021-27252	This vulnerability allows network-adjacent attackers to execute arbitrary code on affected installations of NETGEAR R7800 firmware version 1.0.2.76. Authentication is not required to exploit this vulnerability. The specific flaw exists within the handling of the vendor_specific DHCP opcode. The issue results from the lack of proper validation of a user-supplied string before using it to execute a system call. An attacker can leverage this vulnerability to execute code in the context of root. Was ZDI-CAN-12216.	8.8	More Details

CVE Number	Description	Base Score	Reference
CVE-2021-27253	This vulnerability allows network-adjacent attackers to execute arbitrary code on affected installations of NETGEAR Nighthawk R7800. Although authentication is required to exploit this vulnerability, the existing authentication mechanism can be bypassed. The specific flaw exists within the handling of the rc_service parameter provided to apply_bind.cgi. The issue results from the lack of proper validation of a user-supplied string before using it to execute a system call. An attacker can leverage this vulnerability to execute code in the context of root. Was ZDI-CAN-12303.	8.8	More Details
CVE-2021-30245	The project received a report that all versions of Apache OpenOffice through 4.1.8 can open non-http(s) hyperlinks. The problem has existed since about 2006 and the issue is also in 4.1.9. If the link is specifically crafted this could lead to untrusted code execution. It is always best practice to be careful opening documents from unknown and unverified sources. The mitigation in Apache OpenOffice 4.1.10 (unreleased) assures that a security warning is displayed giving the user the option of continuing to open the hyperlink.	8.8	More Details
CVE-2021-31152	Multilaser Router AC1200 V02.03.01.45_pt contains a cross-site request forgery (CSRF) vulnerability. An attacker can enable remote access, change passwords, and perform other actions through misconfigured requests, entries, and headers.	8.8	More Details
CVE-2021-28242	SQL Injection in the "evoadm.php" component of b2evolution v7.2.2-stable allows remote attackers to obtain sensitive database information by injecting SQL commands into the "cf_name" parameter when creating a new filter under the "Collections" tab.	8.8	More Details
CVE-2021-27394	A vulnerability has been identified in Mendix Applications using Mendix 7 (All versions < V7.23.19), Mendix Applications using Mendix 8 (All versions < V8.17.0), Mendix Applications using Mendix 8 (V8.12) (All versions < V8.12.5), Mendix Applications using Mendix 8 (V8.6) (All versions < V8.6.9), Mendix Applications using Mendix 9 (All versions < V9.0.5). Authenticated, non-administrative users could modify their privileges by manipulating the user role under certain circumstances, allowing them to gain administrative privileges.	8.8	More Details
CVE-2021-3492	Shiftfs, an out-of-tree stacking file system included in Ubuntu Linux kernels, did not properly handle faults occurring during copy_from_user() correctly. These could lead to either a double-free situation or memory not being freed at all. An attacker could use this to cause a denial of service (kernel memory exhaustion) or gain privileges via executing arbitrary code. AKA ZDI-CAN-13562.	8.8	More Details

CVE Number	Description	Base Score	Reference
CVE-2021-28825	The Windows Installation component of TIBCO Software Inc.'s TIBCO Messaging - Eclipse Mosquitto Distribution - Core - Community Edition and TIBCO Messaging - Eclipse Mosquitto Distribution - Core - Enterprise Edition 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 Messaging - Eclipse Mosquitto Distribution - Core - Community Edition: versions 1.3.0 and below and TIBCO Messaging - Eclipse Mosquitto Distribution - Core - Enterprise Edition: versions 1.3.0 and below.	8.8	More Details
CVE-2021-28826	The Windows Installation component of TIBCO Software Inc.'s TIBCO Messaging - Eclipse Mosquitto Distribution - Bridge - Community Edition and TIBCO Messaging - Eclipse Mosquitto Distribution - Bridge - Enterprise Edition 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 Messaging - Eclipse Mosquitto Distribution - Bridge - Community Edition: versions 1.3.0 and below and TIBCO Messaging - Eclipse Mosquitto Distribution - Bridge - Enterprise Edition: versions 1.3.0 and below.	8.8	More Details
CVE-2021-22879	Nextcloud Desktop Client prior to 3.1.3 is vulnerable to resource injection by way of missing validation of URLs, allowing a malicious server to execute remote commands. User interaction is needed for exploitation.	8.8	More Details
CVE-2021-27182	An issue was discovered in MDaemon before 20.0.4. There is an IFRAME injection vulnerability in Webmail (aka WorldClient). It can be exploited via an email message. It allows an attacker to perform any action with the privileges of the attacked user.	8.8	More Details
CVE-2021-27249	This vulnerability allows network-adjacent attackers to execute arbitrary code on affected installations of D-Link DAP-2020 v1.01rc001 Wi-Fi access points. Authentication is not required to exploit this vulnerability. The specific flaw exists within the processing of CGI scripts. The issue results from the lack of proper validation of a user-supplied string before using it to execute a system call. An attacker can leverage this vulnerability to execute code in the context of root. Was ZDI-CAN-11369.	8.8	More Details

CVE Number	Description	Base Score	Reference
CVE-2021-22539	An attacker can place a crafted JSON config file into the project folder pointing to a custom executable. VScode-bazel allows the workspace path to lint *.bzl files to be set via this config file. As such the attacker is able to execute any executable on the system through vscode-bazel. We recommend upgrading to version 0.4.1 or above.	8.2	More Details
CVE-2021-20453	IBM WebSphere Application Server 8.0, 8.5, and 9.0 is vulnerable to a XML External Entity Injection (XXE) attack when processing XML data. A remote attacker could exploit this vulnerability to expose sensitive information or consume memory resources. IBM X-Force ID: 196648.	8.2	More Details
CVE-2020-36323	In the standard library in Rust before 1.52.0, there is an optimization for joining strings that can cause uninitialized bytes to be exposed (or the program to crash) if the borrowed string changes after its length is checked.	8.2	More Details
CVE-2020-28593	A unauthenticated backdoor exists in the configuration server functionality of Cosori Smart 5.8-Quart Air Fryer CS158-AF 1.1.0. A specially crafted JSON object can lead to code execution. An attacker can send a malicious packet to trigger this vulnerability.	8.1	More Details
CVE-2021-29452	a12n-server is an npm package which aims to provide a simple authentication system. A new HAL-Form was added to allow editing users in version 0.18.0. This feature should only have been accessible to admins. Unfortunately, privileges were incorrectly checked allowing any logged in user to make this change. Patched in v0.18.2.	8.1	More Details
CVE-2021-29461	Discord Recon Server is a bot that allows one to do one's reconnaissance process from one's Discord. A vulnerability in Discord Recon Server prior to 0.0.3 could be exploited to read internal files from the system and write files into the system resulting in remote code execution. This issue has been fixed in version 0.0.3. As a workaround, one may copy the code from `assets/CommandInjection.py` in the Discord Recon Server code repository and overwrite vulnerable code from one's own Discord Recon Server implementation with code that contains the patch.	8.1	More Details
CVE-2021-20992	In Fibaro Home Center 2 and Lite devices in all versions provide a web based management interface over unencrypted HTTP protocol. Communication between the user and the device can be eavesdropped to hijack sessions, tokens and passwords.	8.1	More Details

CVE Number	Description	Base Score	Reference
CVE-2021-27246	This vulnerability allows network-adjacent attackers to execute arbitrary code on affected installations of TP-Link Archer A7 AC1750 1.0.15 routers. Authentication is not required to exploit this vulnerability. The specific flaw exists within the handling of MAC addresses by the tdpServer endpoint. A crafted TCP message can write stack pointers to the stack. An attacker can leverage this vulnerability to execute code in the context of the root user. Was ZDI-CAN-12306.	8.0	More Details
CVE-2021-3497	GStreamer before 1.18.4 might access already-freed memory in error code paths when demuxing certain malformed Matroska files.	7.8	More Details
CVE-2021-29279	There is a integer overflow in function filter_core/filter_props.c:gf_props_assign_value in GPAC 1.0.1. In which, the arg const GF_PropertyValue *value,maybe value->value.data.size is a negative number. In result, memcpy in gf_props_assign_value failed.	7.8	More Details
CVE-2021-21094	Adobe Bridge versions 10.1.1 (and earlier) and 11.0.1 (and earlier) are 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.	7.8	More Details
CVE-2021-23887	Privilege Escalation vulnerability in McAfee Data Loss Prevention (DLP) Endpoint for Windows prior to 11.6.100 allows a local, low privileged, attacker to write to arbitrary controlled kernel addresses. This is achieved by launching applications, suspending them, modifying the memory and restarting them when they are monitored by McAfee DLP through the hdlphook driver.	7.8	More Details
CVE-2021-27259	This vulnerability allows local attackers to escalate privileges on affected installations of Parallels Desktop 16.0.1-48919. An attacker must first obtain the ability to execute low-privileged code on the target guest system in order to exploit this vulnerability. The specific flaw exists within the Toolgate component. The issue results from the lack of proper validation of user-supplied data, which can result in an integer overflow before allocating a buffer. An attacker can leverage this vulnerability to escalate privileges and execute arbitrary code in the context of the hypervisor. Was ZDI-CAN-12021.	7.8	More Details
CVE-2021-3498	GStreamer before 1.18.4 might cause heap corruption when parsing certain malformed Matroska files.	7.8	More Details

CVE Number	Description	Base Score	Reference
CVE-2021-21100	Adobe Digital Editions version 4.5.11.187245 (and earlier) is affected by a Privilege Escalation vulnerability during installation. An unauthenticated attacker could leverage this vulnerability to achieve arbitrary file system write 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-2021-27031	A user may be tricked into opening a malicious FBX file which may exploit a use-after-free vulnerability in FBX's Review causing the application to reference a memory location controlled by an unauthorized third party, thereby running arbitrary code on the system.	7.8	More Details
CVE-2021-28549	Adobe Photoshop versions 21.2.6 (and earlier) and 22.3 (and earlier) are affected by a Buffer Overflow vulnerability when parsing a specially crafted JSX 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.	7.8	More Details
CVE-2021-31255	Buffer overflow in the abst_box_read function in MP4Box in GPAC 1.0.1 allows attackers to cause a denial of service or execute arbitrary code via a crafted file.	7.8	More Details
CVE-2021-28098	An issue was discovered in Forescout CounterACT before 8.1.4. A local privilege escalation vulnerability is present in the logging function. SecureConnector runs with administrative privileges and writes logs entries to a file in %PROGRAMDATA%\ForeScout SecureConnector\ that has full permissions for the Everyone group. Using a symbolic link allows an attacker to point the log file to a privileged location such as %WINDIR%\System32. The resulting log file adopts the file permissions of the source of the symbolic link (in this case, the Everyone group). The log file in System32 can be replaced and renamed with a malicious DLL for DLL hijacking.	7.8	More Details
CVE-2021-25314	A Creation of Temporary File With Insecure Permissions vulnerability in hawk2 of SUSE Linux Enterprise High Availability 12-SP3, SUSE Linux Enterprise High Availability 12-SP5, SUSE Linux Enterprise High Availability 15-SP2 allows local attackers to escalate to root. This issue affects: SUSE Linux Enterprise High Availability 12-SP3 hawk2 versions prior to 2.6.3+git.1614685906.812c31e9. SUSE Linux Enterprise High Availability 12-SP5 hawk2 versions prior to 2.6.3+git.1614685906.812c31e9. SUSE Linux Enterprise High Availability 15-SP2 hawk2 versions prior to 2.6.3+git.1614684118.af555ad9.	7.8	More Details

CVE Number	Description	Base Score	Reference
CVE-2021-29457	Exiv2 is a command-line utility and C++ library for reading, writing, deleting, and modifying the metadata of image files. A heap buffer overflow was found in Exiv2 versions v0.27.3 and earlier. The heap overflow is triggered when Exiv2 is used to write metadata into a crafted image file. An attacker could potentially exploit the vulnerability to gain code execution, if they can trick the victim into running Exiv2 on a crafted image file. Note that this bug is only triggered when _writing_ the metadata, which is a less frequently used Exiv2 operation than _reading_ the metadata. For example, to trigger the bug in the Exiv2 command-line application, you need to add an extra command-line argument such as `insert`. The bug is fixed in version v0.27.4.	7.8	More Details
CVE-2020-9668	Adobe Genuine Service version 6.6 (and earlier) is affected by an Improper Access control vulnerability when handling symbolic links. An unauthenticated attacker could exploit this to elevate privileges in the context of the current user.	7.8	More Details
CVE-2020-7851	Innorix Web-Based File Transfer Solution versuibs prior to and including 9.2.18.385 contains a vulnerability that could allow remote files to be downloaded and executed by setting the arguments to the internal method. A remote attacker could induce a user to access a crafted web page, causing damage such as malicious code infection.	7.8	More Details
CVE-2021-21981	VMware NSX-T contains a privilege escalation vulnerability due to an issue with RBAC (Role based access control) role assignment. Successful exploitation of this issue may allow attackers with local guest user account to assign privileges higher than their own permission level.	7.8	More Details
CVE-2021-27027	An Out-Of-Bounds Read Vulnerability in Autodesk FBX Review version 1.5.0 and prior may lead to code execution through maliciously crafted DLL files or information disclosure.	7.8	More Details
CVE-2021-27028	A Memory Corruption Vulnerability in Autodesk FBX Review version 1.5.0 and prior may lead to remote code execution through maliciously crafted DLL files.	7.8	More Details
CVE-2021-27030	A user may be tricked into opening a malicious FBX file which may exploit a Directory Traversal Remote Code Execution vulnerability in FBX's Review causing it to run arbitrary code on the system.	7.8	More Details
CVE-2021-31254	Buffer overflow in the tenc_box_read function in MP4Box in GPAC 1.0.1 allows attackers to cause a denial of service or execute arbitrary code via a crafted file, related invalid IV sizes.	7.8	More Details

CVE Number	Description	Base Score	Reference
CVE-2021-29431	Sydent is a reference Matrix identity server. Sydent can be induced to send HTTP GET requests to internal systems, due to lack of parameter validation or IP address blacklisting. It is not possible to exfiltrate data or control request headers, but it might be possible to use the attack to perform an internal port enumeration. This issue has been addressed in in 9e57334, 8936925, 3d531ed, 0f00412. A potential workaround would be to use a firewall to ensure that Sydent cannot reach internal HTTP resources.	7.7	More Details
CVE-2021-26073	Broken Authentication in Atlassian Connect Express (ACE) from version 3.0.2 before version 6.6.0: Atlassian Connect Express is a Node.js package for building Atlassian Connect apps. Authentication between Atlassian products and the Atlassian Connect Express app occurs with a server-to-server JWT or a context JWT. Atlassian Connect Express versions from 3.0.2 before 6.6.0 erroneously accept context JWTs in lifecycle endpoints (such as installation) where only server-to-server JWTs should be accepted, permitting an attacker to send authenticated re-installation events to an app.	7.7	More Details
CVE-2021-29448	Pi-hole is a Linux network-level advertisement and Internet tracker blocking application. The Stored XSS exists in the Pi-hole Admin portal, which can be exploited by the malicious actor with the network access to DNS server. See the referenced GitHub security advisory for patch details.	7.6	More Details
CVE-2021-29462	The Portable SDK for UPnP Devices is an SDK for development of UPnP device and control point applications. The server part of pupnp (libupnp) appears to be vulnerable to DNS rebinding attacks because it does not check the value of the `Host` header. This can be mitigated by using DNS revolvers which block DNS-rebinding attacks. The vulnerability is fixed in version 1.14.6 and later.	7.6	More Details

CVE Number	Description	Base Score	Reference
CVE-2021-28828	The Administration GUI component of TIBCO Software Inc.'s TIBCO Administrator - Enterprise Edition, TIBCO Administrator - Enterprise Edition, TIBCO Administrator - Enterprise Edition Distribution for TIBCO Silver Fabric, TIBCO Administrator - Enterprise Edition Distribution for TIBCO Silver Fabric, TIBCO Administrator - Enterprise Edition for z/Linux, and TIBCO Administrator - Enterprise Edition for z/Linux contains an easily exploitable vulnerability that allows a low privileged attacker with network access to execute a SQL injection attack on the affected system. Affected releases are TIBCO Software Inc.'s TIBCO Administrator - Enterprise Edition: versions 5.10.2 and below, TIBCO Administrator - Enterprise Edition: versions 5.11.0 and 5.11.1, TIBCO Administrator - Enterprise Edition Distribution for TIBCO Silver Fabric: versions 5.10.2 and below, TIBCO Administrator - Enterprise Edition Distribution for TIBCO Silver Fabric: versions 5.11.0 and 5.11.1, TIBCO Administrator - Enterprise Edition for z/Linux: versions 5.10.2 and below, and TIBCO Administrator - Enterprise Edition for z/Linux: versions 5.11.0 and 5.11.1.	7.6	More Details
CVE-2021-28484	An issue was discovered in the /api/connector endpoint handler in Yubico yubihsm-connector before 3.0.1 (in YubiHSM SDK before 2021.04). The handler did not validate the length of the request, which can lead to a state where yubihsm-connector becomes stuck in a loop waiting for the YubiHSM to send it data, preventing any further operations until the yubihsm-connector is restarted. An attacker can send 0, 1, or 2 bytes to trigger this.	7.5	More Details
CVE-2020-36120	Buffer Overflow in the "sixel_encoder_encode_bytes" function of Libsixel v1.8.6 allows attackers to cause a Denial of Service (DoS).	7.5	More Details
CVE-2021-26827	Buffer Overflow in TP-Link WR2041 v1 firmware for the TL-WR2041+ router allows remote attackers to cause a Denial-of-Service (DoS) by sending an HTTP request with a very long "ssid" parameter to the "/userRpm/popupSiteSurveyRpm.html" webpage, which crashes the router.	7.5	More Details
CVE-2020-26197	Dell PowerScale OneFS 8.1.0 - 9.1.0 contains an LDAP Provider inability to connect over TLSv1.2 vulnerability. It may make it easier to eavesdrop and decrypt such traffic for a malicious actor. Note: This does not affect clusters which are not relying on an LDAP server for the authentication provider.	7.5	More Details
CVE-2021-27608	An unquoted service path in SAPSetup, version - 9.0, could lead to privilege escalation during the installation process that is performed when an executable file is registered. This could further lead to complete compromise of confidentiality, Integrity and Availability.	7.5	More Details

CVE Number	Description	Base Score	Reference
CVE-2021-29455	Grassroot Platform is an application to make it faster, cheaper and easier to persistently organize and mobilize people in low-income communities. Grassroot Platform before master deployment as of 2021-04-16 did not properly verify the signature of JSON Web Tokens when refreshing an existing JWT. This allows to forge a valid JWT. The problem has been patched in version 1.3.1 by deprecating the JWT refresh function, which was an overdue deprecation regardless (the "refresh" flow is no longer used).	7.5	More Details
CVE-2020-7856	A vulnerability of Helpcom could allow an unauthenticated attacker to execute arbitrary command. This vulnerability exists due to insufficient authentication validation.	7.5	More Details
CVE-2021-25681	AdTran Personal Phone Manager 10.8.1 software is vulnerable to an issue that allows for exfiltration of data over DNS. This could allow for exposed AdTran Personal Phone Manager web servers to be used as DNS redirectors to tunnel arbitrary data over DNS. NOTE: The affected appliances NetVanta 7060 and NetVanta 7100 are considered End of Life and as such this issue will not be patched	7.5	More Details
CVE-2021-20990	In Fibaro Home Center 2 and Lite devices with firmware version 4.600 and older an internal management service is accessible on port 8000 and some API endpoints could be accessed without authentication to trigger a shutdown, a reboot or a reboot into recovery mode.	7.5	More Details
CVE-2021-27458	If Ethernet communication of the JTEKT Corporation TOYOPUC product series' (TOYOPUC-PC10 Series: PC10G-CPU TCC-6353: All versions, PC10GE TCC-6464: All versions, PC10P TCC-6372: All versions, PC10P-DP TCC-6726: All versions, PC10P-DP-IO TCC-6752: All versions, PC10B-P TCC-6373: All versions, PC10B TCC-1021: All versions, PC10B-E/C TCU-6521: All versions, PC10E TCC-4737: All versions; TOYOPUC-Plus Series: Plus CPU TCC-6740: All versions, Plus EX TCU-6741: All versions, Plus EX2 TCU-6858: All versions, Plus EFR TCU-6743: All versions, Plus EFR2 TCU-6859: All versions, Plus 2P-EFR TCU-6929: All versions, Plus BUS-EX TCU-6900: All versions; TOYOPUC-PC3J/PC2J Series: FL/ET-T-V2H THU-6289: All versions, 2PORT-EFR THU-6404: All versions) are left in an open state by an attacker, Ethernet communications cannot be established with other devices, depending on the settings of the link parameters.	7.5	More Details
CVE-2021-27990	Appspace 6.2.4 is vulnerable to a broken authentication mechanism where pages such as /medianet/mail.aspx can be called directly and the framework is exposed with layouts, menus and functionalities.	7.5	More Details

CVE Number	Description	Base Score	Reference
CVE-2021-30464	OMICRON StationGuard before 1.10 allows remote attackers to cause a denial of service (connectivity outage) via crafted tcp/20499 packets to the CTRL Ethernet port.	7.5	More Details
CVE-2021-28156	HashiCorp Consul Enterprise version 1.8.0 up to 1.9.4 audit log can be bypassed by specifically crafted HTTP events. Fixed in 1.9.5, and 1.8.10.	7.5	More Details
CVE-2020-7857	A vulnerability of XPlatform could allow an unauthenticated attacker to execute arbitrary command. This vulnerability exists due to insufficient validation of improper classes. This issue affects: Tobesoft XPlatform versions prior to 9.2.2.280.	7.5	More Details
CVE-2021-31402	The dio package 4.0.0 for Dart allows CRLF injection if the attacker controls the HTTP method string, a different vulnerability than CVE-2020-35669.	7.5	More Details
CVE-2021-3017	The web interface on Intelbras WIN 300 and WRN 342 devices through 2021-01-04 allows remote attackers to discover credentials by reading the def_wirelesspassword line in the HTML source code.	7.5	More Details
CVE-2021-29430	Sydent is a reference Matrix identity server. Sydent does not limit the size of requests it receives from HTTP clients. A malicious user could send an HTTP request with a very large body, leading to memory exhaustion and denial of service. Sydent also does not limit response size for requests it makes to remote Matrix homeservers. A malicious homeserver could return a very large response, again leading to memory exhaustion and denial of service. This affects any server which accepts registration requests from untrusted clients. This issue has been patched by releases 89071a1, 0523511, f56eee3. As a workaround request sizes can be limited in an HTTP reverse-proxy. There are no known workarounds for the problem with overlarge responses.	7.5	More Details
CVE-2021-23379	This affects all versions of package portkiller. If (attacker-controlled) user input is given, 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-2021-23374	This affects all versions of package ps-visitor. If attacker-controlled user input is given to the kill 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-2021-23381	This affects all versions of package killing. If attacker-controlled user input is given, 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-2021-23375	This affects all versions of package psnode. If attacker-controlled user input is given to the kill 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-2021-27183	An issue was discovered in MDaemon before 20.0.4. Administrators can use Remote Administration to exploit an Arbitrary File Write vulnerability. An attacker is able to create new files in any location of the filesystem, or he may be able to modify existing files. This vulnerability may directly lead to Remote Code Execution.	7.2	More Details
CVE-2021-20288	An authentication flaw was found in ceph in versions before 14.2.20. When the monitor handles CEPHX_GET_AUTH_SESSION_KEY requests, it doesn't sanitize other_keys, allowing key reuse. An attacker who can request a global_id can exploit the ability of any user to request a global_id previously associated with another user, as ceph does not force the reuse of old keys to generate new ones. The highest threat from this vulnerability is to data confidentiality and integrity as well as system availability.	7.2	More Details
CVE-2021-29654	AjaxSearchPro before 4.20.8 allows Deserialization of Untrusted Data (in the import database feature of the administration panel), leading to Remote Code execution.	7.2	More Details
CVE-2021-20527	IBM Resilient SOAR V38.0 could allow a privileged user to create create malicious scripts that could be executed as another user. IBM X-Force ID: 198759.	7.2	More Details
CVE-2021-28157	An SQL Injection issue in Devolutions Server before 2021.1 and Devolutions Server LTS before 2020.3.18 allows an administrative user to execute arbitrary SQL commands via a username in api/security/userinfo/delete.	7.2	More Details
CVE-2021-29447	Wordpress is an open source CMS. A user with the ability to upload files (like an Author) can exploit an XML parsing issue in the Media Library leading to XXE attacks. This requires WordPress installation to be using PHP 8. Access to internal files is possible in a successful XXE attack. This has been patched in WordPress version 5.7.1, along with the older affected versions via a minor release. We strongly recommend you keep auto-updates enabled.	7.1	More Details

CVE Number	Description	Base Score	Reference
CVE-2021-3506	An out-of-bounds (OOB) memory access flaw was found in fs/f2fs/node.c in the f2fs module in the Linux kernel in versions before 5.12.0-rc4. A bounds check failure allows a local attacker to gain access to out-of-bounds memory leading to a system crash or a leak of internal kernel information. The highest threat from this vulnerability is to system availability.	7.1	More Details
CVE-2021-0488	In pb_write of pb_encode.c, there is a possible out of bounds write due to a missing bounds check. This could lead to local escalation of privilege with System execution privileges needed. User interaction is not needed for exploitation.Product: AndroidVersions: Android kernelAndroid ID: A-178754781	6.7	More Details
CVE-2021-3035	An unsafe deserialization vulnerability in Bridgecrew Checkov by Prisma Cloud allows arbitrary code execution when processing a malicious terraform file. This issue impacts Checkov 2.0 versions earlier than Checkov 2.0.26. Checkov 1.0 versions are not impacted.	6.7	More Details
CVE-2021-30209	Textpattern V4.8.4 contains an arbitrary file upload vulnerability where a plug-in can be loaded in the background without any security verification, which may lead to obtaining system permissions.	6.5	More Details
CVE-2021-29450	Wordpress is an open source CMS. One of the blocks in the WordPress editor can be exploited in a way that exposes password-protected posts and pages. This requires at least contributor privileges. This has been patched in WordPress 5.7.1, along with the older affected versions via minor releases. It's strongly recommended that you keep auto-updates enabled to receive the fix.	6.5	More Details
CVE-2021-31229	An issue was discovered in libezxml.a in ezXML 0.8.6. The function ezxml_internal_dtd() performs incorrect memory handling while parsing crafted XML files, which leads to an out-of-bounds write of a one byte constant.	6.5	More Details
CVE-2021-26074	Broken Authentication in Atlassian Connect Spring Boot (ACSB) from version 1.1.0 before version 2.1.3: Atlassian Connect Spring Boot is a Java Spring Boot package for building Atlassian Connect apps. Authentication between Atlassian products and the Atlassian Connect Spring Boot app occurs with a server-to-server JWT or a context JWT. Atlassian Connect Spring Boot versions from version 1.1.0 before version 2.1.3 erroneously accept context JWTs in lifecycle endpoints (such as installation) where only server-to-server JWTs should be accepted, permitting an attacker to send authenticated re-installation events to an app.	6.5	More Details

CVE Number	Description	Base Score	Reference
CVE-2021-28055	An issue was discovered in Centreon-Web in Centreon Platform 20.10.0. The anti-CSRF token generation is predictable, which might allow CSRF attacks that add an admin user.	6.5	More Details
CVE-2021-27604	In order to prevent XML External Entity vulnerability in SAP NetWeaver ABAP Server and ABAP Platform (Process Integration - Enterprise Service Repository JAVA Mappings), versions - 7.10, 7.20, 7.30, 7.31, 7.40, 7.50, SAP recommends to refer this note.	6.5	More Details
CVE-2021-27247	This vulnerability allows remote attackers to disclose sensitive information on affected installations of Tencent WeChat 2.9.5 desktop version. 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 WXAM decoder. 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 in conjunction with other vulnerabilities to execute arbitrary code in the context of the current process. Was ZDI-CAN-11907.	6.5	More Details
CVE-2021-27599	SAP NetWeaver ABAP Server and ABAP Platform (Process Integration - Integration Builder Framework), versions - 7.10, 7.30, 7.31, 7.40, 7.50, allows an attacker to access information under certain conditions, which would otherwise be restricted.	6.5	More Details
CVE-2021-27250	This vulnerability allows network-adjacent attackers to disclose sensitive information on affected installations of D-Link DAP-2020 v1.01rc001 Wi-Fi access points. Authentication is not required to exploit this vulnerability. The specific flaw exists within the processing of CGI scripts. When parsing the errorpage request parameter, the process does not properly validate a user-supplied path prior to using it in file operations. An attacker can leverage this vulnerability to disclose stored credentials, leading to further compromise. Was ZDI-CAN-11856.	6.5	More Details
CVE-2020-9681	Adobe Genuine Service version 6.6 (and earlier) is affected by an Uncontrolled Search Path element vulnerability. An authenticated attacker could exploit this to rewrite the file of the administrator, which may lead to elevated permissions. Exploitation of this issue requires user interaction.	6.5	More Details
CVE-2021-31347	An issue was discovered in libezxml.a in ezXML 0.8.6. The function ezxml_parse_str() performs incorrect memory handling while parsing crafted XML files (writing outside a memory region created by mmap).	6.5	More Details
CVE-2021-31348	An issue was discovered in libezxml.a in ezXML 0.8.6. The function ezxml_parse_str() performs incorrect memory handling while parsing crafted XML files (out-of-bounds read after a certain strcspn failure).	6.5	More Details

CVE Number	Description	Base Score	Reference
CVE-2021-28048	An overly permissive CORS policy in Devolutions Server before 2021.1 and Devolutions Server LTS before 2020.3.18 allows a remote attacker to leak cross-origin data via a crafted HTML page.	6.5	More Details
CVE-2021-27545	SQL Injection in the "add-services.php" component of PHPGurukul Beauty Parlour Management System v1.0 allows remote attackers to obtain sensitive database information by injecting SQL commands into the "sername" parameter.	6.5	More Details
CVE-2020-9667	Adobe Genuine Service version 6.6 (and earlier) is affected by an Uncontrolled Search Path element vulnerability. An authenticated attacker with admin privileges could plant custom binaries and execute them with System permissions. Exploitation of this issue requires user interaction.	6.5	More Details
CVE-2021-28829	The Administration GUI component of TIBCO Software Inc.'s TIBCO Administrator - Enterprise Edition, TIBCO Administrator - Enterprise Edition, TIBCO Administrator - Enterprise Edition Distribution for TIBCO Silver Fabric, TIBCO Administrator - Enterprise Edition Distribution for TIBCO Silver Fabric, TIBCO Administrator - Enterprise Edition for z/Linux, and TIBCO Administrator - Enterprise Edition for z/Linux contains an easily exploitable vulnerability that allows a low privileged attacker with network access to execute a persistent CSV injection attack from the affected system. A successful attack using this vulnerability requires human interaction from a person other than the attacker. Affected releases are TIBCO Software Inc.'s TIBCO Administrator - Enterprise Edition: versions 5.10.2 and below, TIBCO Administrator - Enterprise Edition: versions 5.11.0 and 5.11.1, TIBCO Administrator - Enterprise Edition Distribution for TIBCO Silver Fabric: versions 5.10.2 and below, TIBCO Administrator - Enterprise Edition Distribution for TIBCO Silver Fabric: versions 5.11.0 and 5.11.1, TIBCO Administrator - Enterprise Edition for z/Linux: versions 5.10.2 and below, and TIBCO Administrator - Enterprise Edition for z/Linux: versions 5.11.0 and 5.11.1.	6.5	More Details
CVE-2021-21070	Adobe Robohelp version 2020.0.3 (and earlier) is affected by an uncontrolled search path element vulnerability that could lead to privilege escalation. An attacker with admin permissions to write to the file system could leverage this vulnerability to escalate privileges.	6.5	More Details
CVE-2021-29449	Pi-hole is a Linux network-level advertisement and Internet tracker blocking application. Multiple privilege escalation vulnerabilities were discovered in version 5.2.4 of Pi-hole core. See the referenced GitHub security advisory for details.	6.3	More Details
CVE-2020-21087	Cross Site Scripting (XSS) in X2Engine X2CRM v6.9 and older allows remote attackers to execute arbitrary code by injecting arbitrary web script or HTML via the "New Name" field of the "Rename a Module" tool.	6.1	More Details

CVE Number	Description	Base Score	Reference
CVE-2021-29434	Wagtail is a Django content management system. In affected versions of Wagtail, when saving the contents of a rich text field in the admin interface, Wagtail does not apply server-side checks to ensure that link URLs use a valid protocol. A malicious user with access to the admin interface could thus craft a POST request to publish content with `javascript:` URLs containing arbitrary code. The vulnerability is not exploitable by an ordinary site visitor without access to the Wagtail admin. See referenced GitHub advisory for additional details, including a workaround. Patched versions have been released as Wagtail 2.11.7 (for the LTS 2.11 branch) and Wagtail 2.12.4 (for the current 2.12 branch).	6.1	More Details
CVE-2018-19942	A cross-site scripting (XSS) vulnerability has been reported to affect earlier versions of File Station. If exploited, this vulnerability allows remote attackers to inject malicious code. We have already fixed this vulnerability in the following versions: QTS 4.5.2.1566 build 20210202 (and later) QTS 4.5.1.1456 build 20201015 (and later) QTS 4.3.6.1446 build 20200929 (and later) QTS 4.3.4.1463 build 20201006 (and later) QTS 4.3.3.1432 build 20201006 (and later) QTS 4.2.6 build 20210327 (and later) QuTS hero h4.5.1.1472 build 20201031 (and later) QuTScloud c4.5.4.1601 build 20210309 (and later) QuTScloud c4.5.3.1454 build 20201013 (and later)	6.1	More Details
CVE-2021-29399	XMB is vulnerable to cross-site scripting (XSS) due to inadequate filtering of BBCode input. This bug affects all versions of XMB. All XMB installations must be updated to versions 1.9.12.03 or 1.9.11.16.	6.1	More Details
CVE-2021-26832	Cross Site Scripting (XSS) in the "Reset Password" page form of Priority Enterprise Management System v8.00 allows attackers to execute javascript on behalf of the victim by sending a malicious URL or directing the victim to a malicious site.	6.1	More Details
CVE-2021-27288	Cross Site Scripting (XSS) in X2Engine X2CRM v7.1 allows remote attackers to obtain sensitive information by injecting arbitrary web script or HTML via the "Comment" field in "/profile/activity" page.	6.1	More Details
CVE-2021-26812	Cross Site Scripting (XSS) in the Jitsi Meet 2.7 through 2.8.3 plugin for Moodle via the "sessionpriv.php" module. This allows attackers to craft a malicious URL, which when clicked on by users, can inject javascript code to be run by the application.	6.1	More Details

CVE Number	Description	Base Score	Reference
CVE-2021-26582	A security vulnerability in HPE IceWall SSO Domain Gateway Option (Dgfw) module version 10.0 on RHEL 5/6/7, version 10.0 on HP-UX 11i v3, version 10.0 on Windows and 11.0 on Windows could be exploited remotely to allow cross-site scripting (XSS).	6.1	More Details
CVE-2020-35419	Cross Site Scripting (XSS) in Group Office CRM 6.4.196 via the SET_LANGUAGE parameter.	6.1	More Details
CVE-2021-3243	Wfilter ICF 5.0.117 contains a cross-site scripting (XSS) vulnerability. An attacker in the same LAN can craft a packet with a malicious User-Agent header to inject a payload in its logs, where an attacker can take over the system by through its plugin-running function.	6.1	More Details
CVE-2021-27180	An issue was discovered in MDaemon before 20.0.4. There is Reflected XSS in Webmail (aka WorldClient). It can be exploited via a GET request. It allows performing any action with the privileges of the attacked user.	6.1	More Details
CVE-2021-26030	An issue was discovered in Joomla! 3.0.0 through 3.9.25. Inadequate escaping allowed XSS attacks using the logo parameter of the default templates on error page	6.1	More Details
CVE-2021-25680	The AdTran Personal Phone Manager software is vulnerable to multiple reflected cross-site scripting (XSS) issues. These issues impact at minimum versions 10.8.1 and below but potentially impact later versions as well since they have not previously been disclosed. Only version 10.8.1 was able to be confirmed during primary research. NOTE: The affected appliances NetVanta 7060 and NetVanta 7100 are considered End of Life and as such this issue will not be patched	6.1	More Details
CVE-2020-36288	The issue navigation and search view in Jira Server and Data Center before version 8.5.12, from version 8.6.0 before version 8.13.4, and from version 8.14.0 before version 8.15.1 allows remote attackers to inject arbitrary HTML or JavaScript via a DOM Cross-Site Scripting (XSS) vulnerability caused by parameter pollution.	6.1	More Details
CVE-2021-20208	A flaw was found in cifs-utils in versions before 6.13. A user when mounting a krb5 CIFS file system from within a container can use Kerberos credentials of the host. The highest threat from this vulnerability is to data confidentiality and integrity.	6.1	More Details
CVE-2020-25864	HashiCorp Consul and Consul Enterprise up to version 1.9.4 key-value (KV) raw mode was vulnerable to cross-site scripting. Fixed in 1.9.5, 1.8.10 and 1.7.14.	6.1	More Details

CVE Number	Description	Base Score	Reference
CVE-2021-1079	NVIDIA GeForce Experience, all versions prior to 3.22, contains a vulnerability in GameStream plugins where log files are created using NT/System level permissions, which may lead to code execution, denial of service, or local privilege escalation. The attacker does not have control over the consequence of a modification nor would they be able to leak information as a direct result of the overwrite.	6.1	More Details
CVE-2021-21526	Dell PowerScale OneFS 8.1.0 - 9.1.0 contains a privilege escalation in SmartLock compliance mode that may allow compadmin to execute arbitrary commands as root.	6.0	More Details
CVE-2021-29445	jose-node-esm-runtime is an npm package which provides a number of cryptographic functions. In versions prior to 3.11.4 the AES_CBC_HMAC_SHA2 Algorithm (A128CBC-HS256, A192CBC-HS384, A256CBC-HS512) decryption would always execute both HMAC tag verification and CBC decryption, if either failed `JWEDecryptionFailed` would be thrown. But a possibly observable difference in timing when padding error would occur while decrypting the ciphertext makes a padding oracle and an adversary might be able to make use of that oracle to decrypt data without knowing the decryption key by issuing on average 128*b calls to the padding oracle (where b is the number of bytes in the ciphertext block). A patch was released which ensures the HMAC tag is verified before performing CBC decryption. The fixed versions are `>=3.11.4`. Users should upgrade to `^3.11.4`.	5.9	More Details
CVE-2018-25008	In the standard library in Rust before 1.29.0, there is weak synchronization in the Arc::get_mut method. This synchronization issue can be lead to memory safety issues through race conditions.	5.9	More Details
CVE-2021-20989	Fibaro Home Center 2 and Lite devices with firmware version 4.600 and older initiate SSH connections to the Fibaro cloud to provide remote access and remote support capabilities. This connection can be intercepted using DNS spoofing attack and a device initiated remote port-forward channel can be used to connect to the web management interface. Knowledge of authorization credentials to the management interface is required to perform any further actions.	5.9	More Details

CVE Number	Description	Base Score	Reference
CVE-2021-21405	Lotus is an Implementation of the Filecoin protocol written in Go. BLS signature validation in lotus uses blst library method VerifyCompressed. This method accepts signatures in 2 forms: "serialized", and "compressed", meaning that BLS signatures can be provided as either of 2 unique byte arrays. Lotus block validation functions perform a uniqueness check on provided blocks. Two blocks are considered distinct if the CIDs of their blockheader do not match. The CID method for blockheader includes the BlockSig of the block. The result of these issues is that it would be possible to punish miners for valid blocks, as there are two different valid block CIDs available for each block, even though this must be unique. By switching from the go based `blst` bindings over to the bindings in `filecoin-ffi`, the code paths now ensure that all signatures are compressed by size and the way they are deserialized. This happened in https://github.com/filecoin-project/lotus/pull/5393.	5.9	More Details
CVE-2021-29446	jose-node-cjs-runtime is an npm package which provides a number of cryptographic functions. In versions prior to 3.11.4 the AES_CBC_HMAC_SHA2 Algorithm (A128CBC-HS256, A192CBC-HS384, A256CBC-HS512) decryption would always execute both HMAC tag verification and CBC decryption, if either failed `JWEDecryptionFailed` would be thrown. But a possibly observable difference in timing when padding error would occur while decrypting the ciphertext makes a padding oracle and an adversary might be able to make use of that oracle to decrypt data without knowing the decryption key by issuing on average 128*b calls to the padding oracle (where b is the number of bytes in the ciphertext block). A patch was released which ensures the HMAC tag is verified before performing CBC decryption. The fixed versions are `>=3.11.4`. Users should upgrade to `^3.11.4`.	5.9	More Details
CVE-2017-20004	In the standard library in Rust before 1.19.0, there is a synchronization problem in the MutexGuard object. MutexGuards can be used across threads with any types, allowing for memory safety issues through race conditions.	5.9	More Details

CVE Number	Description	Base Score	Reference
CVE-2021-29444	jose-browser-runtime is an npm package which provides a number of cryptographic functions. In versions prior to 3.11.4 the AES_CBC_HMAC_SHA2 Algorithm (A128CBC-HS256, A192CBC-HS384, A256CBC-HS512) decryption would always execute both HMAC tag verification and CBC decryption, if either failed `JWEDecryptionFailed` would be thrown. But a possibly observable difference in timing when padding error would occur while decrypting the ciphertext makes a padding oracle and an adversary might be able to make use of that oracle to decrypt data without knowing the decryption key by issuing on average 128*b calls to the padding oracle (where b is the number of bytes in the ciphertext block). A patch was released which ensures the HMAC tag is verified before performing CBC decryption. The fixed versions are `>=3.11.4`. Users should upgrade to `^3.11.4`.	5.9	More Details
CVE-2021-29443	jose is an npm library providing a number of cryptographic operations. In vulnerable versions AES_CBC_HMAC_SHA2 Algorithm (A128CBC-HS256, A192CBC-HS384, A256CBC-HS512) decryption would always execute both HMAC tag verification and CBC decryption, if either failed `JWEDecryptionFailed` would be thrown. A possibly observable difference in timing when padding error would occur while decrypting the ciphertext makes a padding oracle and an adversary might be able to make use of that oracle to decrypt data without knowing the decryption key by issuing on average 128*b calls to the padding oracle (where b is the number of bytes in the ciphertext block). All major release versions have had a patch released which ensures the HMAC tag is verified before performing CBC decryption. The fixed versions are `^1.28.1 || ^2.0.5 || >=3.11.4`. Users should upgrade their v1.x dependency to ^1.28.1, their v2.x dependency to ^2.0.5, and their v3.x dependency to ^3.11.4. Thanks to Jason from Microsoft Vulnerability Research (MSVR) for bringing this up and Eva Sarafianou (@esarafianou) for helping to score this advisory.	5.9	More Details
CVE-2021-30496	The Telegram app 7.6.2 for iOS allows remote authenticated users to cause a denial of service (application crash) if the victim pastes an attacker-supplied message (e.g., in the Persian language) into a channel or group. The crash occurs in MtProtoKitFramework. NOTE: the vendor's perspective is that "this behavior can't be considered a vulnerability."	5.7	More Details

CVE Number	Description	Base Score	Reference
CVE-2021-29453	matrix-media-repo is an open-source multi-domain media repository for Matrix. Versions 1.2.6 and earlier of matrix-media-repo do not properly handle malicious images which are crafted to be small in file size, but large in complexity. A malicious user could upload a relatively small image in terms of file size, using particular image formats, which expands to have extremely large dimensions during the process of thumbnailing. The server can be exhausted of memory in the process of trying to load the whole image into memory for thumbnailing, leading to denial of service. Version 1.2.7 has a fix for the vulnerability.	5.7	More Details
CVE-2021-23380	This affects all versions of package roar-pidusage. If attacker-controlled user input is given to the stat function of this package on certain operating systems, it is possible for an attacker to execute arbitrary commands. This is due to use of the child_process exec function without input sanitization.	5.6	More Details
CVE-2021-31259	The gf_isom_cenc_get_default_info_internal function in GPAC 1.0.1 allows attackers to cause a denial of service (NULL pointer dereference) via a crafted file in the MP4Box command.	5.5	More Details
CVE-2021-29458	Exiv2 is a command-line utility and C++ library for reading, writing, deleting, and modifying the metadata of image files. An out-of-bounds read was found in Exiv2 versions v0.27.3 and earlier. The out-of-bounds read is triggered when Exiv2 is used to write metadata into a crafted image file. An attacker could potentially exploit the vulnerability to cause a denial of service by crashing Exiv2, if they can trick the victim into running Exiv2 on a crafted image file. Note that this bug is only triggered when writing the metadata, which is a less frequently used Exiv2 operation than reading the metadata. For example, to trigger the bug in the Exiv2 command-line application, you need to add an extra command-line argument such as insert. The bug is fixed in version v0.27.4.	5.5	More Details
CVE-2021-29155	An issue was discovered in the Linux kernel through 5.11.x. kernel/bpf/verifier.c performs undesirable out-of-bounds speculation on pointer arithmetic, leading to side-channel attacks that defeat Spectre mitigations and obtain sensitive information from kernel memory. Specifically, for sequences of pointer arithmetic operations, the pointer modification performed by the first operation is not correctly accounted for when restricting subsequent operations.	5.5	More Details
CVE-2021-31256	Memory leak in the stbl_GetSampleInfos function in MP4Box in GPAC 1.0.1 allows attackers to read memory via a crafted file.	5.5	More Details

CVE Number	Description	Base Score	Reference
CVE-2021-31257	The HintFile function in GPAC 1.0.1 allows attackers to cause a denial of service (NULL pointer dereference) via a crafted file in the MP4Box command.	5.5	More Details
CVE-2021-3038	A denial-of-service (DoS) vulnerability in Palo Alto Networks GlobalProtect app on Windows systems allows a limited Windows user to send specifically-crafted input to the GlobalProtect app that results in a Windows blue screen of death (BSOD) error. This issue impacts: GlobalProtect app 5.1 versions earlier than GlobalProtect app 5.1.8; GlobalProtect app 5.2 versions earlier than GlobalProtect app 5.2.4.	5.5	More Details
CVE-2021-31258	The gf_isom_set_extraction_slc function in GPAC 1.0.1 allows attackers to cause a denial of service (NULL pointer dereference) via a crafted file in the MP4Box command.	5.5	More Details
CVE-2021-30199	In filters/reframe_latm.c in GPAC 1.0.1 there is a Null Pointer Dereference, when gf_filter_pck_get_data is called. The first arg pck may be null with a crafted mp4 file,which results in a crash.	5.5	More Details
CVE-2021-3505	A flaw was found in libtpms in versions before 0.8.0. The TPM 2 implementation returns 2048 bit keys with ~1984 bit strength due to a bug in the TCG specification. The bug is in the key creation algorithm in RsaAdjustPrimeCandidate(), which is called before the prime number check. The highest threat from this vulnerability is to data confidentiality.	5.5	More Details
CVE-2021-31261	The gf_hinter_track_new function in GPAC 1.0.1 allows attackers to read memory via a crafted file in the MP4Box command.	5.5	More Details
CVE-2021-30022	There is a integer overflow in media_tools/av_parsers.c in the gf_avc_read_pps_bs_internal in GPAC 1.0.1. pps_id may be a negative number, so it will not return. However, avc->pps only has 255 unit, so there is an overflow, which results a crash.	5.5	More Details
CVE-2021-30020	In the function gf_hevc_read_pps_bs_internal function in media_tools/av_parsers.c in GPAC 1.0.1 there is a loop, which with crafted file, pps->num_tile_columns may be larger than sizeof(pps->column_width), which results in a heap overflow in the loop.	5.5	More Details
CVE-2020-14105	The application in the mobile phone can read the SNO information of the device, Xiaomi 10 MIUI < 2020.01.15.	5.5	More Details

CVE Number	Description	Base Score	Reference
CVE-2021-30019	In the adts_dmx_process function in filters/reframe_adts.c in GPAC 1.0.1, a crafted file may cause ctx->hdr.frame_size to be smaller than ctx->hdr.hdr_size, resulting in size to be a negative number and a heap overflow in the memcpy.	5.5	More Details
CVE-2021-30014	There is a integer overflow in media_tools/av_parsers.c in the hevc_parse_slice_segment function in GPAC 1.0.1 which results in a crash.	5.5	More Details
CVE-2021-31260	The MergeTrack function in GPAC 1.0.1 allows attackers to cause a denial of service (NULL pointer dereference) via a crafted file in the MP4Box command.	5.5	More Details
CVE-2021-31262	The AV1_DuplicateConfig function in GPAC 1.0.1 allows attackers to cause a denial of service (NULL pointer dereference) via a crafted file in the MP4Box command.	5.5	More Details
CVE-2021-30015	There is a Null Pointer Dereference in function filter_core/filter_pck.c:gf_filter_pck_new_alloc_internal in GPAC 1.0.1. The pid comes from function av1dmx_parse_flush_sample, the ctx.opid maybe NULL. The result is a crash in gf_filter_pck_new_alloc_internal.	5.5	More Details
CVE-2020-36322	An issue was discovered in the FUSE filesystem implementation in the Linux kernel before 5.10.6, aka CID-5d069dbe8aaf. fuse_do_getattr() calls make_bad_inode() in inappropriate situations, causing a system crash. NOTE: the original fix for this vulnerability was incomplete, and its incompleteness is tracked as CVE-2021-28950.	5.5	More Details
CVE-2021-27029	The user may be tricked into opening a malicious FBX file which may exploit a Null Pointer Dereference vulnerability in FBX's Review version 1.5.0 and prior causing the application to crash leading to a denial of service.	5.5	More Details
CVE-2021-26805	Buffer Overflow in tsMuxer 2.6.16 allows attackers to cause a Denial of Service (DoS) by running the application with a malicious WAV file.	5.5	More Details
CVE-2021-27815	NULL Pointer Deference in the exif command line tool, when printing out XML formatted EXIF data, in exif v0.6.22 and earlier allows attackers to cause a Denial of Service (DoS) by uploading a malicious JPEG file, causing the application to crash.	5.5	More Details
CVE-2021-29338	Integer Overflow in OpenJPEG v2.4.0 allows remote attackers to crash the application, causing a Denial of Service (DoS). This occurs when the attacker uses the command line option "-ImgDir" on a directory that contains 1048576 files.	5.5	More Details

CVE Number	Description	Base Score	Reference
CVE-2021-23886	Denial of Service vulnerability in McAfee Data Loss Prevention (DLP) Endpoint for Windows prior to 11.6.100 allows a local, low privileged, attacker to cause a BSoD through suspending a process, modifying the processes memory and restarting it. This is triggered by the hdlphook driver reading invalid memory.	5.5	More Details
CVE-2021-30493	Multiple system services installed alongside the Razer Synapse 3 software suite perform privileged operations on entries within the ChromaBroadcast subkey. These privileged operations consist of file name concatenation of a runtime log file that is used to store runtime log information. In other words, an attacker can create a file in an unintended directory (with some limitations).	5.5	More Details
CVE-2021-30494	Multiple system services installed alongside the Razer Synapse 3 software suite perform privileged operations on entries within the Razer Chroma SDK subkey. These privileged operations consist of file name concatenation of a runtime log file that is used to store runtime log information. In other words, an attacker can create a file in an unintended directory (with some limitations).	5.5	More Details
CVE-2021-21096	Adobe Bridge versions 10.1.1 (and earlier) and 11.0.1 (and earlier) are affected by an Improper Authorization vulnerability in the Genuine Software Service. A low-privileged attacker could leverage this vulnerability to achieve application denial-of-service in the context of the current user. Exploitation of this issue does not require user interaction.	5.5	More Details
CVE-2021-28855	In Deark before 1.5.8, a specially crafted input file can cause a NULL pointer dereference in the dbuf_write function (src/deark-dbuf.c).	5.5	More Details
CVE-2021-28856	In Deark before v1.5.8, a specially crafted input file can cause a division by zero in (src/fmtutil.c) because of the value of pixelsize.	5.5	More Details
CVE-2021-21087	Adobe Coldfusion versions 2016 (update 16 and earlier), 2018 (update 10 and earlier) and 2021.0.0.323925 are affected by an Improper Neutralization of Input During Web Page Generation ('Cross-site Scripting') vulnerability. An attacker could abuse this vulnerability to execute arbitrary JavaScript code in context of the current user. Exploitation of this issue requires user interaction.	5.4	More Details

CVE Number	Description	Base Score	Reference
CVE-2021-25679	The AdTran Personal Phone Manager software is vulnerable to an authenticated stored cross-site scripting (XSS) issues. These issues impact at minimum versions 10.8.1 and below but potentially impact later versions as well since they have not previously been disclosed. Only version 10.8.1 was able to be confirmed during primary research. NOTE: The affected appliances NetVanta 7060 and NetVanta 7100 are considered End of Life and as such this issue will not be patched	5.4	More Details
CVE-2021-27129	CASAP Automated Enrollment System version 1.0 contains a cross-site scripting (XSS) vulnerability through the Students > Edit > ROUTE parameter.	5.4	More Details
CVE-2020-35660	Cross Site Scripting (XSS) in Monica before 2.19.1 via the journal page.	5.4	More Details
CVE-2020-28141	The messaging subsystem in the Online Discussion Forum 1.0 is vulnerable to XSS in the message body. An authenticated user can send messages to arbitrary users on the system that include javascript that will execute when viewing the messages page.	5.4	More Details
CVE-2020-28124	Cross Site Scripting (XSS) in LavaLite 5.8.0 via the Address field.	5.4	More Details
CVE-2020-35418	Cross Site Scripting (XSS) in the contact page of Group Office CRM 6.4.196 by uploading a crafted svg file.	5.4	More Details
CVE-2020-29593	An issue was discovered in Orchard before 1.10. The Media Settings Allowed File Types list field allows an attacker to add a XSS payload that will execute when users attempt to upload a disallowed file type, causing the error to display.	5.4	More Details
CVE-2021-27989	Appspace 6.2.4 is vulnerable to stored cross-site scripting (XSS) in multiple parameters within /medianet/sgcontentset.aspx.	5.4	More Details
CVE-2021-30479	An issue was discovered in Zulip Server before 3.4. A bug in the implementation of the all_public_streams API feature resulted in guest users being able to receive message traffic to public streams that should have been only accessible to members of the organization.	5.3	More Details
CVE-2021-26031	An issue was discovered in Joomla! 3.0.0 through 3.9.25. Inadequate filters on module layout settings could lead to an LFI.	5.3	More Details

CVE Number	Description	Base Score	Reference
CVE-2021-28060	A Server-Side Request Forgery (SSRF) vulnerability in Group Office 6.4.196 allows a remote attacker to forge GET requests to arbitrary URLs via the url parameter to group/api/upload.php.	5.3	More Details
CVE-2020-28898	In QED ResourceXpress through 4.9k, a large numeric or alphanumeric value submitted in specific URL parameters causes a server error in script execution due to insufficient input validation.	5.3	More Details
CVE-2021-29432	Sydent is a reference matrix identity server. A malicious user could abuse Sydent to send out arbitrary emails from the Sydent email address. This could be used to construct plausible phishing emails, for example. This issue has been fixed in 4469d1d.	5.3	More Details
CVE-2021-28492	Unisys Stealth (core) 5.x before 5.0.048.0, 5.1.x before 5.1.017.0, and 6.x before 6.0.037.0 stores passwords in a recoverable format.	4.9	More Details
CVE-2020-7270	Exposure of Sensitive Information in the web interface in McAfee Advanced Threat Defense (ATD) prior to 4.12.2 allows remote authenticated users to view sensitive unencrypted information via a carefully crafted HTTP request parameter. The risk is partially mitigated if your ATD instances are deployed as recommended with no direct access from the Internet to them.	4.9	More Details
CVE-2021-27672	SQL Injection in the "admin_boxes.ajax.php" component of Tribal Systems Zenario CMS v8.8.52729 allows remote attackers to obtain sesnitive database information by injecting SQL commands into the "cID" parameter when creating a new HTML component.	4.9	More Details
CVE-2020-7269	Exposure of Sensitive Information in the web interface in McAfee Advanced Threat Defense (ATD) prior to 4.12.2 allows remote authenticated users to view sensitive unencrypted information via a carefully crafted HTTP request parameter. The risk is partially mitigated if your ATD instances are deployed as recommended with no direct access from the Internet to them.	4.9	More Details
CVE-2021-20023	SonicWall Email Security version 10.0.9.x contains a vulnerability that allows a post-authenticated attacker to read an arbitrary file on the remote host.	4.9	More Details
CVE-2021-27673	Cross Site Scripting (XSS) in the "admin_boxes.ajax.php" component of Tribal Systems Zenario CMS v8.8.52729 allows remote attackers to execute arbitrary code by injecting arbitrary HTML into the "cID" parameter when creating a new HTML component.	4.8	More Details

CVE Number	Description	Base Score	Reference
CVE-2020-7308	Cleartext Transmission of Sensitive Information between McAfee Endpoint Security (ENS) for Windows prior to 10.7.0 February 2021 Update and McAfee Global Threat Intelligence (GTI) servers using DNS allows a remote attacker to view the requests from ENS and responses from GTI over DNS. By gaining control of an intermediate DNS server or altering the network DNS configuration, it is possible for an attacker to intercept requests and send their own responses.	4.8	More Details
CVE-2020-21088	Cross Site Scripting (XSS) in X2engine X2CRM v7.1 and older allows remote attackers to obtain sensitive information by injecting arbitrary web script or HTML via the "First Name" and "Last Name" fields in "/index.php/contacts/create page"	4.8	More Details
CVE-2021-27544	Cross Site Scripting (XSS) in the "add-services.php" component of PHPGurukul Beauty Parlour Management System v1.0 allows remote attackers to execute arbitrary code by injecting arbitrary HTML into the "sername" parameter.	4.8	More Details
CVE-2021-20491	IBM Spectrum Protect Server 7.1 and 8.1 is subject to a stack-based buffer overflow caused by improper bounds checking during the parsing of commands. By issuing such a command with an improper parameter, an authorized administrator could overflow a buffer and cause the server to crash. IBM X-Force ID: 197792.	4.4	More Details
CVE-2021-3036	An information exposure through log file vulnerability exists in Palo Alto Networks PAN-OS software where secrets in PAN-OS XML API requests are logged in cleartext to the web server logs when the API is used incorrectly. This vulnerability applies only to PAN-OS appliances that are configured to use the PAN-OS XML API and exists only when a client includes a duplicate API parameter in API requests. Logged information includes the cleartext username, password, and API key of the administrator making the PAN-OS XML API request.	4.4	More Details
CVE-2021-30477	An issue was discovered in Zulip Server before 3.4. A bug in the implementation of replies to messages sent by outgoing webhooks to private streams meant that an outgoing webhook bot could be used to send messages to private streams that the user was not intended to be able to send messages to.	4.3	More Details
CVE-2021-29433	Sydent is a reference Matrix identity server. In Sydent versions 2.2.0 and prior, sissing input validation of some parameters on the endpoints used to confirm third-party identifiers could cause excessive use of disk space and memory leading to resource exhaustion. A patch for the vulnerability is in version 2.3.0. No workarounds are known to exist.	4.3	More Details

CVE Number	Description	Base Score	Reference
CVE-2021-26075	The Jira importers plugin AttachTemporaryFile rest resource in Jira Server and Data Center before version 8.5.12, from version 8.6.0 before 8.13.4, and from version 8.14.0 before 8.15.1 allowed remote authenticated attackers to obtain the full path of the Jira application data directory via an information disclosure vulnerability in the error message when presented with an invalid filename.	4.3	More Details
CVE-2021-30478	An issue was discovered in Zulip Server before 3.4. A bug in the implementation of the can_forge_sender permission (previously is_api_super_user) resulted in users with this permission being able to send messages appearing as if sent by a system bot, including to other organizations hosted by the same Zulip installation.	4.3	More Details
CVE-2021-23884	Cleartext Transmission of Sensitive Information vulnerability in the ePO Extension of McAfee Content Security Reporter (CSR) prior to 2.8.0 allows an ePO administrator to view the unencrypted password of the McAfee Web Gateway (MWG) or the password of the McAfee Web Gateway Cloud Server (MWGCS) read only user used to retrieve log files for analysis in CSR.	4.3	More Details
CVE-2021-26076	The jira.editor.user.mode cookie set by the Jira Editor Plugin in Jira Server and Data Center before version 8.5.12, from version 8.6.0 before version 8.13.4, and from version 8.14.0 before version 8.15.0 allows remote anonymous attackers who can perform an attacker in the middle attack to learn which mode a user is editing in due to the cookie not being set with a secure attribute if Jira was configured to use https.	3.7	More Details
CVE-2021-25316	A Insecure Temporary File vulnerability in s390-tools of SUSE Linux Enterprise Server 12-SP5, SUSE Linux Enterprise Server 15-SP2 allows local attackers to prevent VM live migrations This issue affects: SUSE Linux Enterprise Server 12-SP5 s390-tools versions prior to 2.1.0-18.29.1. SUSE Linux Enterprise Server 15-SP2 s390-tools versions prior to 2.11.0-9.20.1.	3.3	More Details
CVE-2021-27260	This vulnerability allows local attackers to disclose sensitive information on affected installations of Parallels Desktop 16.0.1-48919. An attacker must first obtain the ability to execute high-privileged code on the target guest system in order to exploit this vulnerability. The specific flaw exists within the Toolgate component. 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 in conjunction with other vulnerabilities to escalate privileges and execute arbitrary code in the context of the hypervisor. Was ZDI-CAN-12068.	3.2	More Details

CVE Number	Description	Base Score	Reference
CVE-2021-30487	In the topic moving API in Zulip Server 3.x before 3.4, organization administrators were able to move messages to streams in other organizations hosted by the same Zulip installation.	2.7	More Details
CVE-2021-3037	An information exposure through log file vulnerability exists in Palo Alto Networks PAN-OS software where the connection details for a scheduled configuration export are logged in system logs. Logged information includes the cleartext username, password, and IP address used to export the PAN-OS configuration to the destination server.	2.3	More Details
CVE-2021-3487	Rejected reason: Non Security Issue. See the binutils security policy for more details, https://sourceware.org/cgit/binutils-gdb/tree/binutils/SECURITY.txt	N/A	More Details
CVE-2021-30138	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-2021-28548	Adobe Photoshop versions 21.2.6 (and earlier) and 22.3 (and earlier) are affected by a Buffer Overflow vulnerability when parsing a specially crafted JSX 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.	N/A	More Details
CVE-2021-21095	Adobe Bridge versions 10.1.1 (and earlier) and 11.0.1 (and earlier) are affected by an Out-of-bounds write vulnerability when parsing a 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.	N/A	More Details
CVE-2021-21092	Adobe Bridge versions 10.1.1 (and earlier) and 11.0.1 (and earlier) are affected by a memory corruption 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.	N/A	More Details
CVE-2021-21091	Adobe Bridge versions 10.1.1 (and earlier) and 11.0.1 (and earlier) are affected by an Out-of-bounds read vulnerability when parsing a crafted file. An unauthenticated attacker could leverage this vulnerability to disclose sensitive memory information in the context of the current user. Exploitation of this issue requires user interaction in that a victim must open a malicious file.	N/A	More Details

CVE Number	Description	Base Score	Reference
CVE-2021-21093	Adobe Bridge versions 10.1.1 (and earlier) and 11.0.1 (and earlier) are affected by a memory corruption 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.	N/A	More Details