SingCERT
Singapore Cyber Emergency Response Team

Security Bulletin 23 February 2022

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

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

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

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

CRITICAL VULNERABILITIES

CVE Number	Description	Base Score	Reference
CVE-2022-21215	This vulnerability could allow an attacker to force the server to create and execute a web request granting access to backend APIs that are only accessible to the Mimosa MMP server, or request pages that could perform some actions themselves. The attacker could force the server into accessing routes on those cloud-hosting platforms, accessing secret keys, changing configurations, etc. Affecting MMP: All versions prior to v1.0.3, PTP C-series: Device versions prior to v2.8.6.1, and PTMP C-series and A5x: Device versions prior to v2.5.4.1.	10.0	More Details
CVE-2022-21141	MMP: All versions prior to v1.0.3, PTP C-series: Device versions prior to v2.8.6.1, and PTMP C-series and A5x: Device versions prior to v2.5.4.1 does not perform proper authorization checks on multiple API functions. An attacker may gain access to these functions and achieve remote code execution, create a denial-of-service condition, and obtain sensitive information.	10.0	More Details
CVE-2022-21196	MMP: All versions prior to v1.0.3, PTP C-series: Device versions prior to v2.8.6.1, and PTMP C-series and A5x: Device versions prior to v2.5.4.1 does not perform proper authorization and authentication checks on multiple API routes. An attacker may gain access to these API routes and achieve remote code execution, create a denial-of-service condition, and obtain sensitive information.	10.0	More Details
CVE-2022-0543	It was discovered, that redis, a persistent key-value database, due to a packaging issue, is prone to a (Debian-specific) Lua sandbox escape, which could result in remote code execution.	10.0	More Details

CVE Number	Description	Base Score	Reference
CVE-2022-24663	PHP Everywhere <= 2.0.3 included functionality that allowed execution of PHP Code Snippets via WordPress shortcodes, which can be used by any authenticated user.	9.9	More Details
CVE-2022-24664	PHP Everywhere <= 2.0.3 included functionality that allowed execution of PHP Code Snippets via WordPress metaboxes, which could be used by any user able to edit posts.	9.9	More Details
CVE-2022-24665	PHP Everywhere <= 2.0.3 included functionality that allowed execution of PHP Code Snippets via a WordPress gutenberg block by any user able to edit posts.	9.9	More Details
CVE-2021-3781	A trivial sandbox (enabled with the `-dSAFER` option) escape flaw was found in the ghostscript interpreter by injecting a specially crafted pipe command. This flaw allows a specially crafted document to execute arbitrary commands on the system in the context of the ghostscript interpreter. The highest threat from this vulnerability is to confidentiality, integrity, as well as system availability.	9.9	More Details
CVE-2021-46036	An arbitrary file upload vulnerability in the component /ms/file/uploadTemplate.do of MCMS v5.2.4 allows attackers to execute arbitrary code.	9.8	More Details
CVE-2021-46110	Online Shopping Portal v3.1 was discovered to contain multiple time-based SQL injection vulnerabilities via the email and contactno parameters.	9.8	More Details
CVE-2022-24049	This vulnerability allows remote attackers to execute arbitrary code on affected installations of Sonos One Speaker prior to 3.4.1 (S2 systems) and 11.2.13 build 57923290 (S1 systems). Authentication is not required to exploit this vulnerability. The specific flaw exists within the ALAC audio codec. 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 root. Was ZDI-CAN-15798.	9.8	More Details
CVE-2022-24047	This vulnerability allows remote attackers to bypass authentication on affected installations of BMC Track-It! 20.21.01.102. Authentication is not required to exploit this vulnerability. The specific flaw exists within the authorization of HTTP requests. The issue results from the lack of authentication prior to allowing access to functionality. An attacker can leverage this vulnerability to bypass authentication on the system. Was ZDI-CAN-14618.	9.8	More Details
CVE-2022-25235	xmltok_impl.c in Expat (aka libexpat) before 2.4.5 lacks certain validation of encoding, such as checks for whether a UTF-8 character is valid in a certain context.	9.8	More Details
CVE-2022-25337	Ibexa DXP ezsystems/ezpublish-kernel 7.5.x before 7.5.26 and 1.3.x before 1.3.12 allows injection attacks via image filenames.	9.8	More Details
CVE-2021-29656	Pexip Infinity Connect before 1.8.0 mishandles TLS certificate validation. The allow list is not properly checked.	9.8	More Details

CVE Number	Description	Base Score	Reference
CVE-2021-45401	A Command injection vulnerability exists in Tenda AC10U AC1200 Smart Dual-band Wireless Router AC10U V1.0 Firmware V15.03.06.49_multi via the setUsbUnload functionality. The vulnerability is caused because the client controlled "deviceName" value is passed directly to the "doSystemCmd" function.	9.8	More Details
CVE-2021-3657	A flaw was found in mbsync versions prior to 1.4.4. Due to inadequate handling of extremely large (>=2GiB) IMAP literals, malicious or compromised IMAP servers, and hypothetically even external email senders, could cause several different buffer overflows, which could conceivably be exploited for remote code execution.	9.8	More Details
CVE-2021-29655	Pexip Infinity Connect before 1.8.0 omits certain provisioning authenticity checks. Thus, untrusted code may execute.	9.8	More Details
CVE-2022-25132	A command injection vulnerability in the function meshSlaveDlfw of TOTOLINK Technology router T6 V3_Firmware T6_V3_V4.1.5cu.748_B20211015 allows attackers to execute arbitrary commands via a crafted MQTT packet.	9.8	More Details
CVE-2022-25130	A command injection vulnerability in the function updateWifiInfo of TOTOLINK Technology routers T6 V3_Firmware T6_V3_V4.1.5cu.748_B20211015 and T10 V2_Firmware V4.1.8cu.5207_B20210320 allows attackers to execute arbitrary commands via a crafted MQTT packet.	9.8	More Details
CVE-2022-25131	A command injection vulnerability in the function recvSlaveCloudCheckStatus of TOTOLINK Technology routers T6 V3_Firmware T6_V3_V4.1.5cu.748_B20211015 and T10 V2_Firmware V4.1.8cu.5207_B20210320 allows attackers to execute arbitrary commands via a crafted MQTT packet.	9.8	More Details
CVE-2022-25322	ZEROF Web Server 2.0 allows /HandleEvent SQL Injection.	9.8	More Details
CVE-2022-25133	A command injection vulnerability in the function isAssocPriDevice of TOTOLINK Technology router T6 V3_Firmware T6_V3_V4.1.5cu.748_B20211015 allows attackers to execute arbitrary commands via a crafted MQTT packet.	9.8	More Details
CVE-2022-25134	A command injection vulnerability in the function setUpgradeFW of TOTOLINK Technology router T6 V3_Firmware T6_V3_V4.1.5cu.748_B20211015 allows attackers to execute arbitrary commands via a crafted MQTT packet.	9.8	More Details
CVE-2022-25135	A command injection vulnerability in the function recv_mesh_info_sync of TOTOLINK Technology router T6 V3_Firmware T6_V3_V4.1.5cu.748_B20211015 allows attackers to execute arbitrary commands via a crafted MQTT packet.	9.8	More Details
CVE-2022-25136	A command injection vulnerability in the function meshSlaveUpdate of TOTOLINK Technology routers T6 V3_Firmware T6_V3_V4.1.5cu.748_B20211015 and T10 V2_Firmware V4.1.8cu.5207_B20210320 allows attackers to execute arbitrary commands via a crafted MQTT packet.	9.8	More Details
CVE-2022-25137	A command injection vulnerability in the function recvSlaveUpgstatus of TOTOLINK Technology routers T6 V3_Firmware T6_V3_V4.1.5cu.748_B20211015 and T10 V2_Firmware V4.1.8cu.5207_B20210320 allows attackers to execute arbitrary commands via a crafted MQTT packet.	9.8	More Details

CVE Number	Description	Base Score	Reference
CVE-2016-1239	duck before 0.10 did not properly handle loading of untrusted code from the current directory.	9.8	More Details
CVE-2022-23848	In Alluxio before 2.7.3, the logserver does not validate the input stream. NOTE: this is not the same as the CVE-2021-44228 Log4j vulnerability.	9.8	More Details
CVE-2022-0691	Authorization Bypass Through User-Controlled Key in NPM url-parse prior to 1.5.9.	9.8	More Details
CVE-2021-24867	Numerous Plugins and Themes from the AccessPress Themes (aka Access Keys) vendor are backdoored due to their website being compromised. Only plugins and themes downloaded via the vendor website are affected, and those hosted on wordpress.org are not. However, all of them were updated or removed to avoid any confusion	9.8	More Details
CVE-2022-24553	An issue was found in Zfaka <= 1.4.5. The verification of the background file upload function check is not strict, resulting in remote command execution.	9.8	More Details
CVE-2021-20325	Missing fixes for CVE-2021-40438 and CVE-2021-26691 in the versions of httpd, as shipped in Red Hat Enterprise Linux 8.5.0, causes a security regression compared to the versions shipped in Red Hat Enterprise Linux 8.4. A user who installs or updates to Red Hat Enterprise Linux 8.5.0 would be vulnerable to the mentioned CVEs, even if they were properly fixed in Red Hat Enterprise Linux 8.4. CVE-2021-20325 was assigned to that Red Hat specific security regression and it does not affect the upstream versions of httpd.	9.8	More Details
CVE-2022-0664	Use of Hard-coded Cryptographic Key in Go github.com/gravitl/netmaker prior to 0.8.5,0.9.4,0.10.0,0.10.1.	9.8	More Details
CVE-2022-25236	xmlparse.c in Expat (aka libexpat) before 2.4.5 allows attackers to insert namespace-separator characters into namespace URIs.	9.8	More Details
CVE-2022-24984	Forms generated by JQueryForm.com before 2022-02-05 (if file-upload capability is enabled) allow remote unauthenticated attackers to upload executable files and achieve remote code execution. This occurs because file-extension checks occur on the client side, and because not all executable content (e.g., .phtml or .php.bak) is blocked.	9.8	More Details
CVE-2022-0559	Use After Free in GitHub repository radareorg/radare2 prior to 5.6.2.	9.8	More Details
CVE-2022-23358	EasyCMS v1.6 allows for SQL injection via ArticlemAction.class.php. In the background, search terms provided by the user were not sanitized and were used directly to construct a SQL statement.	9.8	More Details

CVE Number	Description	Base Score	Reference
CVE-2022-0513	The WP Statistics WordPress plugin is vulnerable to SQL Injection due to insufficient escaping and parameterization of the exclusion_reason parameter found in the ~/includes/class-wp-statistics-exclusion.php file which allows attackers without authentication to inject arbitrary SQL queries to obtain sensitive information, in versions up to and including 13.1.4. This requires the "Record Exclusions" option to be enabled on the vulnerable site.	9.8	More Details
CVE-2022-24086	Adobe Commerce versions 2.4.3-p1 (and earlier) and 2.3.7-p2 (and earlier) are affected by an improper input validation vulnerability during the checkout process. Exploitation of this issue does not require user interaction and could result in arbitrary code execution.	9.8	More Details
CVE-2021-3773	A flaw in netfilter could allow a network-connected attacker to infer openvpn connection endpoint information for further use in traditional network attacks.	9.8	More Details
CVE-2021-3242	DuxCMS v3.1.3 was discovered to contain a SQL injection vulnerability via the component s/tools/SendTpl/index?keyword=.	9.8	More Details
CVE-2021-43299	Stack overflow in PJSUA API when calling pjsua_player_create. An attacker-controlled 'filename' argument may cause a buffer overflow since it is copied to a fixed-size stack buffer without any size validation.	9.8	More Details
CVE-2021-43300	Stack overflow in PJSUA API when calling pjsua_recorder_create. An attacker-controlled 'filename' argument may cause a buffer overflow since it is copied to a fixed-size stack buffer without any size validation.	9.8	More Details
CVE-2021-43301	Stack overflow in PJSUA API when calling pjsua_playlist_create. An attacker-controlled 'file_names' argument may cause a buffer overflow since it is copied to a fixed-size stack buffer without any size validation.	9.8	More Details
CVE-2021-43303	Buffer overflow in PJSUA API when calling pjsua_call_dump. An attacker-controlled 'buffer' argument may cause a buffer overflow, since supplying an output buffer smaller than 128 characters may overflow the output buffer, regardless of the 'maxlen' argument supplied	9.8	More Details
CVE-2022-22880	Jeecg-boot v3.0 was discovered to contain a SQL injection vulnerability via the code parameter in /jeecg-boot/sys/user/queryUserByDepId.	9.8	More Details
CVE-2022-22881	Jeecg-boot v3.0 was discovered to contain a SQL injection vulnerability via the code parameter in /sys/user/queryUserComponentData.	9.8	More Details
CVE-2022-0631	Heap-based Buffer Overflow in Homebrew mruby prior to 3.2.	9.8	More Details
CVE-2022-22885	Hutool v5.7.18's HttpRequest was discovered to ignore all TLS/SSL certificate validation.	9.8	More Details

CVE Number	Description	Base Score	Reference
CVE-2021-44868	A problem was found in ming-soft MCMS v5.1. There is a sql injection vulnerability in /ms/cms/content/list.do	9.8	More Details
CVE-2022-22912	Prototype pollution vulnerability via .parse() in Plist before v3.0.4 allows attackers to cause a Denial of Service (DoS) and may lead to remote code execution.	9.8	More Details
CVE-2021-45382	A Remote Command Execution (RCE) vulnerability exists in all series H/W revisions D-link DIR-810L, DIR-820L/LW, DIR-826L, DIR-830L, and DIR-836L routers via the DDNS function in ncc2 binary file. Note: DIR-810L, DIR-820L, DIR-830L, DIR-826L, DIR-836L, all hardware revisions, have reached their End of Life ("EOL") /End of Service Life ("EOS") Life-Cycle and as such this issue will not be patched.	9.8	More Details
CVE-2021-46314	A Remote Command Execution (RCE) vulnerability exists in HNAP1/control/SetNetworkTomographySettings.php of D-Link Router DIR-846 DIR846A1_FW100A43.bin and DIR846enFW100A53DLA-Retail.bin because backticks can be used for command injection when judging whether it is a reasonable domain name.	9.8	More Details
CVE-2021-46315	Remote Command Execution (RCE) vulnerability exists in HNAP1/control/SetWizardConfig.php in D-Link Router DIR-846 DIR846A1_FW100A43.bin and DIR846enFW100A53DLA-Retail.bin. Malicoius users can use this vulnerability to use "\ " or backticks in the shell metacharacters in the ssid0 or ssid1 parameters to cause arbitrary command execution. Since CVE-2019-17510 vulnerability has not been patched and improved www/hnap1/control/setwizardconfig.php, can also use line breaks and backquotes to bypass.	9.8	More Details
CVE-2021-46319	Remote Code Execution (RCE) vulnerability exists in D-Link Router DIR-846 DIR846A1_FW100A43.bin and DIR846enFW100A53DLA-Retail.bin. Malicious users can use this vulnerability to use "\ " or backticks to bypass the shell metacharacters in the ssid0 or ssid1 parameters to execute arbitrary commands.This vulnerability is due to the fact that CVE-2019-17509 is not fully patched and can be bypassed by using line breaks or backticks on its basis.	9.8	More Details
CVE-2022-22916	O2OA v6.4.7 was discovered to contain a remote code execution (RCE) vulnerability via /x_program_center/jaxrs/invoke.	9.8	More Details
CVE-2022-22922	TP-Link TL-WA850RE Wi-Fi Range Extender before v6_200923 was discovered to use highly predictable and easily detectable session keys, allowing attackers to gain administrative privileges.	9.8	More Details
CVE-2022-25315	In Expat (aka libexpat) before 2.4.5, there is an integer overflow in storeRawNames.	9.8	More Details
CVE-2022-25299	This affects the package cesanta/mongoose before 7.6. The unsafe handling of file names during upload using mg_http_upload() method may enable attackers to write files to arbitrary locations outside the designated target folder.	9.8	More Details

CVE Number	Description	Base Score	Reference
CVE-2021-27797	Brocade Fabric OS before Brocade Fabric OS v8.2.1c, v8.1.2h, and all versions of Brocade Fabric OS v8.0.x and v7.x contain documented hard-coded credentials, which could allow attackers to gain access to the system.	9.8	More Details
CVE-2022-0623	Out-of-bounds Read in Homebrew mruby prior to 3.2.	9.1	More Details
CVE-2021-43302	Read out-of-bounds in PJSUA API when calling pjsua_recorder_create. An attacker-controlled 'filename' argument may cause an out-of-bounds read when the filename is shorter than 4 characters.	9.1	More Details
CVE-2021-46063	MCMS v5.2.5 was discovered to contain a Server Side Template Injection (SSTI) vulnerability via the Template Management module.	9.1	More Details
CVE-2022-0686	Authorization Bypass Through User-Controlled Key in NPM url-parse prior to 1.5.8.	9.1	More Details
CVE-2022-0671	A flaw was found in vscode-xml in versions prior to 0.19.0. Schema download could lead to blind SSRF or DoS via a large file.	9.1	More Details

OTHER VULNERABILITIES

CVE Number	Description	Base Score	Reference
CVE-2020-25718	A flaw was found in the way samba, as an Active Directory Domain Controller, is able to support an RODC (read-only domain controller). This would allow an RODC to print administrator tickets.	8.8	More Details
CVE-2022-23652	capsule-proxy is a reverse proxy for Capsule Operator which provides multi-tenancy in Kubernetes. In versions prior to 0.2.1 an attacker with a proper authentication mechanism may use a malicious `Connection` header to start a privilege escalation attack towards the Kubernetes API Server. This vulnerability allows for an exploit of the `cluster-admin` Role bound to `capsule-proxy`. There are no known workarounds for this issue.	8.8	More Details
CVE-2021-44142	The Samba vfs_fruit module uses extended file attributes (EA, xattr) to provide "...enhanced compatibility with Apple SMB clients and interoperability with a Netatalk 3 AFP fileserver." Samba versions prior to 4.13.17, 4.14.12 and 4.15.5 with vfs_fruit configured allow out-of-bounds heap read and write via specially crafted extended file attributes. A remote attacker with write access to extended file attributes can execute arbitrary code with the privileges of smbd, typically root.	8.8	More Details
CVE-2021-45008	Plesk CMS 18.0.37 is affected by an insecure permissions vulnerability that allows privilege Escalation from user to admin rights. OTE: the vendor states that this is only a site-specific problem on websites of one or more Plesk users	8.8	More Details

CVE Number	Description	Base Score	Reference
CVE-2022-25241	In FileCloud before 21.3, the CSV user import functionality is vulnerable to Cross-Site Request Forgery (CSRF).	8.8	More Details
CVE-2022-0134	The AnyComment WordPress plugin before 0.2.18 does not have CSRF checks in the Import and Revert HyperComments features, allowing attackers to make logged in admin perform such actions via a CSRF attack	8.8	More Details
CVE-2022-24367	This vulnerability allows remote attackers to execute arbitrary code on affected installations of Foxit PDF Reader 11.1.0.52543. 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 handling of AcroForms. 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-15877.	8.8	More Details
CVE-2022-24354	This vulnerability allows network-adjacent attackers to execute arbitrary code on affected installations of TP-Link AC1750 prior to 1.1.4 Build 20211022 rel.59103(5553) routers. Authentication is not required to exploit this vulnerability. The specific flaw exists within the NetUSB.ko module. 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 execute code in the context of root. Was ZDI-CAN-15835.	8.8	More Details
CVE-2022-23644	BookWyrm is a decentralized social network for tracking reading habits and reviewing books. The functionality to load a cover via url is vulnerable to a server-side request forgery attack. Any BookWyrm instance running a version prior to v0.3.0 is susceptible to attack from a logged-in user. The problem has been patched and administrators should upgrade to version 0.3.0 As a workaround, BookWyrm instances can close registration and limit members to trusted individuals.	8.8	More Details
CVE-2022-24355	This vulnerability allows network-adjacent attackers to execute arbitrary code on affected installations of TP-Link TL-WR940N 3.20.1 Build 200316 Rel.34392n (5553) routers. Authentication is not required to exploit this vulnerability. The specific flaw exists within the parsing of file name extensions. The issue results from the lack of proper validation of 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-13910.	8.8	More Details
CVE-2021-25082	The Popup Builder WordPress plugin before 4.0.7 does not validate and sanitise the sgpb_type parameter before using it in a require statement, leading to a Local File Inclusion issue. Furthermore, since the beginning of the string can be controlled, the issue can lead to RCE vulnerability via wrappers such as PHAR	8.8	More Details
CVE-2022-24356	This vulnerability allows remote attackers to execute arbitrary code on affected installations of Foxit PDF Reader Foxit reader 11.0.1.0719 macOS. 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 OnMouseExit method. 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 object. An attacker can leverage this vulnerability to execute code in the context of the current process. Was ZDI-CAN-14848.	8.8	More Details

CVE Number	Description	Base Score	Reference
CVE-2021-25069	The Download Manager WordPress plugin before 3.2.34 does not sanitise and escape the package_ids parameter before using it in a SQL statement, leading to a SQL injection, which can also be exploited to cause a Reflected Cross-Site Scripting issue	8.8	More Details
CVE-2022-24985	Forms generated by JQueryForm.com before 2022-02-05 allows a remote authenticated attacker to bypass authentication and access the administrative section of other forms hosted on the same web server. This is relevant only when an organization hosts more than one of these forms on their server.	8.8	More Details
CVE-2022-24357	This vulnerability allows remote attackers to execute arbitrary code on affected installations of Foxit PDF Reader 11.1.0.52543. 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 handling of Annotation objects. 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-15743.	8.8	More Details
CVE-2022-23375	WikiDocs version 0.1.18 has an authenticated remote code execution vulnerability. An attacker can upload a malicious file using the image upload form through index.php.	8.8	More Details
CVE-2021-41599	A remote code execution vulnerability was identified in GitHub Enterprise Server that could be exploited when building a GitHub Pages site. To exploit this vulnerability, an attacker would need permission to create and build a GitHub Pages site on the GitHub Enterprise Server instance. This vulnerability affected all versions of GitHub Enterprise Server prior to 3.3 and was fixed in versions 3.0.21, 3.1.13, 3.2.5. This vulnerability was reported via the GitHub Bug Bounty program.	8.8	More Details
CVE-2021-44302	BaiCloud-cms v2.5.7 was discovered to contain multiple SQL injection vulnerabilities via the tongji and baidu_map parameters in /user/ztconfig.php.	8.8	More Details
CVE-2022-23642	Sourcegraph is a code search and navigation engine. Sourcegraph prior to version 3.37 is vulnerable to remote code execution in the `gitserver` service. The service acts as a git exec proxy, and fails to properly restrict calling `git config`. This allows an attacker to set the git `core.sshCommand` option, which sets git to use the specified command instead of ssh when they need to connect to a remote system. Exploitation of this vulnerability depends on how Sourcegraph is deployed. An attacker able to make HTTP requests to internal services like gitserver is able to exploit it. This issue is patched in Sourcegraph version 3.37. As a workaround, ensure that requests to gitserver are properly protected.	8.8	More Details
CVE-2022-24358	This vulnerability allows remote attackers to execute arbitrary code on affected installations of Foxit PDF Reader 11.1.0.52543. 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 handling of Doc objects. By performing actions in JavaScript, an attacker can trigger 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-15703.	8.8	More Details

CVE Number	Description	Base Score	Reference
CVE-2022-24359	This vulnerability allows remote attackers to execute arbitrary code on affected installations of Foxit PDF Reader 11.1.0.52543. 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 handling of Doc objects. 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-15702.	8.8	More Details
CVE-2022-24360	This vulnerability allows remote attackers to execute arbitrary code on affected installations of Foxit PDF Reader 11.1.0.52543. 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 handling of Doc objects. 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-15744.	8.8	More Details
CVE-2022-24361	This vulnerability allows remote attackers to execute arbitrary code on affected installations of Foxit PDF Reader 11.1.0.52543. 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 JPEG2000 images. 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 structure. An attacker can leverage this vulnerability to execute code in the context of the current process. Was ZDI-CAN-15811.	8.8	More Details
CVE-2022-24362	This vulnerability allows remote attackers to execute arbitrary code on affected installations of Foxit PDF Reader 11.1.0.52543. 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 AcroForms. 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-15987.	8.8	More Details
CVE-2022-24363	This vulnerability allows remote attackers to execute arbitrary code on affected installations of Foxit PDF Reader 11.1.0.52543. 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 handling of Annotation objects. 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-15861.	8.8	More Details
CVE-2021-4093	A flaw was found in the KVM's AMD code for supporting the Secure Encrypted Virtualization-Encrypted State (SEV-ES). A KVM guest using SEV-ES can trigger out-of-bounds reads and writes in the host kernel via a malicious VMGEXIT for a string I/O instruction (for example, outs or ins) using the exit reason SVM_EXIT_IOIO. This issue results in a crash of the entire system or a potential guest-to-host escape scenario.	8.8	More Details

CVE Number	Description	Base Score	Reference
CVE-2022-24971	This vulnerability allows remote attackers to execute arbitrary code on affected installations of Foxit PDF Reader 11.1.0.52543. 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 JPEG2000 images. 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 structure. An attacker can leverage this vulnerability to execute code in the context of the current process. Was ZDI-CAN-15812.	8.8	More Details
CVE-2022-24364	This vulnerability allows remote attackers to execute arbitrary code on affected installations of Foxit PDF Reader 11.1.0.52543. 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 handling of Doc objects. 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-15851.	8.8	More Details
CVE-2020-25722	Multiple flaws were found in the way samba AD DC implemented access and conformance checking of stored data. An attacker could use this flaw to cause total domain compromise.	8.8	More Details
CVE-2022-24365	This vulnerability allows remote attackers to execute arbitrary code on affected installations of Foxit PDF Reader 11.1.0.52543. 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 handling of AcroForms. 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-15852.	8.8	More Details
CVE-2022-24366	This vulnerability allows remote attackers to execute arbitrary code on affected installations of Foxit PDF Reader 11.1.0.52543. 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 handling of AcroForms. 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-15853.	8.8	More Details
CVE-2022-24295	Okta Advanced Server Access Client for Windows prior to version 1.57.0 was found to be vulnerable to command injection via a specially crafted URL.	8.8	More Details
CVE-2022-24369	This vulnerability allows remote attackers to execute arbitrary code on affected installations of Foxit PDF Reader 11.1.0.52543. 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 JP2 images. Crafted data in a JP2 image can trigger 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-16087.	8.8	More Details
CVE-2022-25242	In FileCloud before 21.3, file upload is not protected against Cross-Site Request Forgery (CSRF).	8.8	More Details

CVE Number	Description	Base Score	Reference
CVE-2022-24046	This vulnerability allows network-adjacent attackers to execute arbitrary code on affected installations of Sonos One Speaker prior to 3.4.1 (S2 systems) and 11.2.13 build 57923290 (S1 systems). Authentication is not required to exploit this vulnerability. The specific flaw exists within the anacapd daemon. The issue results from the lack of proper validation of user-supplied data, which can result in an integer underflow before writing to memory. An attacker can leverage this vulnerability to execute code in the context of root. Was ZDI-CAN-15828.	8.8	More Details
CVE-2021-39297	Potential vulnerabilities have been identified in UEFI firmware (BIOS) for some PC products which may allow escalation of privilege and arbitrary code execution.	8.8	More Details
CVE-2021-39298	A potential vulnerability in AMD System Management Mode (SMM) interrupt handler may allow an attacker with high privileges to access the SMM resulting in arbitrary code execution which could be used by malicious actors to bypass security mechanisms provided in the UEFI firmware.	8.8	More Details
CVE-2021-39299	Potential vulnerabilities have been identified in UEFI firmware (BIOS) for some PC products which may allow escalation of privilege and arbitrary code execution.	8.8	More Details
CVE-2021-39300	Potential vulnerabilities have been identified in UEFI firmware (BIOS) for some PC products which may allow escalation of privilege and arbitrary code execution.	8.8	More Details
CVE-2021-39301	Potential vulnerabilities have been identified in UEFI firmware (BIOS) for some PC products which may allow escalation of privilege and arbitrary code execution.	8.8	More Details
CVE-2021-26726	A remote code execution vulnerability affecting a Valmet DNA service listening on TCP port 1517, allows an attacker to execute commands with SYSTEM privileges This issue affects: Valmet DNA versions from Collection 2012 until Collection 2021.	8.8	More Details
CVE-2022-21176	MMP: All versions prior to v1.0.3, PTP C-series: Device versions prior to v2.8.6.1, and PTMP C-series and A5x: Device versions prior to v2.5.4.1 does not properly sanitize user input, which may allow an attacker to perform a SQL injection and obtain sensitive information.	8.6	More Details
CVE-2021-4120	snapd 2.54.2 fails to perform sufficient validation of snap content interface and layout paths, resulting in the ability for snaps to inject arbitrary AppArmor policy rules via malformed content interface and layout declarations and hence escape strict snap confinement. Fixed in snapd versions 2.54.3+18.04, 2.54.3+20.04 and 2.54.3+21.10.1	8.2	More Details
CVE-2020-8107	A Process Control vulnerability in ProductAgentUI.exe as used in Bitdefender Antivirus Plus allows an attacker to tamper with product settings via a specially crafted DLL file. This issue affects: Bitdefender Antivirus Plus versions prior to 24.0.26.136. Bitdefender Internet Security versions prior to 24.0.26.136. Bitdefender Total Security versions prior to 24.0.26.136.	8.2	More Details

CVE Number	Description	Base Score	Reference
CVE-2022-23654	Wiki.js is a wiki app built on Node.js. In affected versions an authenticated user with write access on a restricted set of paths can update a page outside the allowed paths by specifying a different target page ID while keeping the path intact. The access control incorrectly check the path access against the user-provided values instead of the actual path associated to the page ID. Commit https://github.com/Requarks/wiki/commit/411802ec2f654bb5ed1126c307575b81e2361c6b fixes this vulnerability by checking access control on the path associated with the page ID instead of the user-provided value. When the path is different than the current value, a second access control check is then performed on the user-provided path before the move operation.	8.1	More Details
CVE-2021-46037	MCMS v5.2.4 was discovered to contain an arbitrary file deletion vulnerability via the component /template/unzip.do.	8.1	More Details
CVE-2020-25717	A flaw was found in the way Samba maps domain users to local users. An authenticated attacker could use this flaw to cause possible privilege escalation.	8.1	More Details
CVE-2022-23608	PJSIP is a free and open source multimedia communication library written in C language implementing standard based protocols such as SIP, SDP, RTP, STUN, TURN, and ICE. In versions up to and including 2.11.1 when in a dialog set (or forking) scenario, a hash key shared by multiple UAC dialogs can potentially be prematurely freed when one of the dialogs is destroyed . The issue may cause a dialog set to be registered in the hash table multiple times (with different hash keys) leading to undefined behavior such as dialog list collision which eventually leading to endless loop. A patch is available in commit db3235953baa56d2fb0e276ca510fefca751643f which will be included in the next release. There are no known workarounds for this issue.	8.1	More Details
CVE-2021-46638	This vulnerability allows remote attackers to execute arbitrary code on affected installations of Bentley MicroStation CONNECT 10.16.0.80. 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 DGN 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-15510.	7.8	More Details
CVE-2021-46571	This vulnerability allows remote attackers to execute arbitrary code on affected installations of Bentley View 10.16.0.80. 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 JT 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-15365.	7.8	More Details
CVE-2021-46565	This vulnerability allows remote attackers to execute arbitrary code on affected installations of Bentley MicroStation CONNECT 10.16.0.80. 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 JT 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-15024.	7.8	More Details

CVE Number	Description	Base Score	Reference
CVE-2021-46566	This vulnerability allows remote attackers to execute arbitrary code on affected installations of Bentley MicroStation CONNECT 10.16.0.80. 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 JT files. The issue results from the lack of proper initialization of memory prior to accessing it. An attacker can leverage this vulnerability to execute code in the context of the current process. Was ZDI-CAN-15027.	7.8	More Details
CVE-2021-46567	This vulnerability allows remote attackers to execute arbitrary code on affected installations of Bentley MicroStation CONNECT 10.16.0.80. 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 JT 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-15028.	7.8	More Details
CVE-2021-46568	This vulnerability allows remote attackers to execute arbitrary code on affected installations of Bentley MicroStation CONNECT 10.16.0.80. 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 JT files. Crafted data in a JT file can trigger 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-15030.	7.8	More Details
CVE-2021-46569	This vulnerability allows remote attackers to execute arbitrary code on affected installations of Bentley MicroStation CONNECT 10.16.0.80. 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 JT files. Crafted data in a JT file can trigger 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-15031.	7.8	More Details
CVE-2021-46570	This vulnerability allows remote attackers to disclose sensitive information on affected installations of Bentley View 10.16.0.80. 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 JT files. The issue results from the lack of proper initialization of memory prior to accessing it. An attacker can leverage this in conjunction with other vulnerabilities to execute arbitrary code in the context of the current process. Was ZDI-CAN-15364.	7.8	More Details
CVE-2021-46573	This vulnerability allows remote attackers to execute arbitrary code on affected installations of Bentley MicroStation CONNECT 10.16.0.80. 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 JT 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-15367.	7.8	More Details
CVE-2021-46572	This vulnerability allows remote attackers to execute arbitrary code on affected installations of Bentley MicroStation CONNECT 10.16.0.80. 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 JT files. Crafted data in a JT file can trigger 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-15366.	7.8	More Details

CVE Number	Description	Base Score	Reference
CVE-2021-46574	This vulnerability allows remote attackers to execute arbitrary code on affected installations of Bentley MicroStation CONNECT 10.16.0.80. 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 JT files. Crafted data in a JT file can trigger 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-15368.	7.8	More Details
CVE-2021-46575	This vulnerability allows remote attackers to execute arbitrary code on affected installations of Bentley MicroStation CONNECT 10.16.0.80. 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 DGN 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-15369.	7.8	More Details
CVE-2021-46576	This vulnerability allows remote attackers to execute arbitrary code on affected installations of Bentley MicroStation CONNECT 10.16.0.80. 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 JT files. Crafted data in a JT file can trigger 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-15370.	7.8	More Details
CVE-2021-46577	This vulnerability allows remote attackers to execute arbitrary code on affected installations of Bentley MicroStation CONNECT 10.16.0.80. 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 JT files. The issue results from the lack of proper validation of the length of user-supplied data prior to copying it to a heap-based buffer. An attacker can leverage this vulnerability to execute code in the context of the current process. Was ZDI-CAN-15371.	7.8	More Details
CVE-2021-46652	This vulnerability allows remote attackers to execute arbitrary code on affected installations of Bentley View 10.15.0.75. 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 DGN files. Crafted data in a DGN file can trigger 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-15538.	7.8	More Details
CVE-2021-46578	This vulnerability allows remote attackers to execute arbitrary code on affected installations of Bentley MicroStation CONNECT 10.16.0.80. 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 JT 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-15372.	7.8	More Details
CVE-2021-46643	This vulnerability allows remote attackers to execute arbitrary code on affected installations of Bentley View 10.15.0.75. 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 DGN 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-15515.	7.8	More Details

CVE Number	Description	Base Score	Reference
CVE-2021-46631	This vulnerability allows remote attackers to execute arbitrary code on affected installations of Bentley View 10.15.0.75. 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 images. The issue results from the lack of proper initialization of memory prior to accessing it. An attacker can leverage this vulnerability to execute code in the context of the current process. Was ZDI-CAN-15461.	7.8	More Details
CVE-2022-0646	A flaw use after free in the Linux kernel Management Component Transport Protocol (MCTP) subsystem was found in the way user triggers cancel_work_sync after the unregister_netdev during removing device. A local user could use this flaw to crash the system or escalate their privileges on the system. It is actual from Linux Kernel 5.17-rc1 (when mctp-serial.c introduced) till 5.17-rc5.	7.8	More Details
CVE-2021-46633	This vulnerability allows remote attackers to execute arbitrary code on affected installations of Bentley MicroStation CONNECT 10.16.0.80. 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 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-15463.	7.8	More Details
CVE-2021-46647	This vulnerability allows remote attackers to execute arbitrary code on affected installations of Bentley MicroStation CONNECT 10.16.0.80. 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 images. The issue results from the lack of proper validation of the length of user-supplied data prior to copying it to a heap-based buffer. An attacker can leverage this vulnerability to execute code in the context of the current process. Was ZDI-CAN-15533.	7.8	More Details
CVE-2021-46636	This vulnerability allows remote attackers to execute arbitrary code on affected installations of Bentley MicroStation CONNECT 10.16.0.80. 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 DGN files. Crafted data in a DGN file can trigger 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-15508.	7.8	More Details
CVE-2021-46639	This vulnerability allows remote attackers to execute arbitrary code on affected installations of Bentley MicroStation CONNECT 10.16.0.80. 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 DGN files. Crafted data in a DGN file can trigger 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-15511.	7.8	More Details
CVE-2021-46640	This vulnerability allows remote attackers to execute arbitrary code on affected installations of Bentley View 10.15.0.75. 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 DGN files. Crafted data in a DGN file can trigger 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-15512.	7.8	More Details

CVE Number	Description	Base Score	Reference
CVE-2021-46635	This vulnerability allows remote attackers to execute arbitrary code on affected installations of Bentley MicroStation CONNECT 10.16.0.80. 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 DGN files. Crafted data in a DGN file can trigger 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-15507.	7.8	More Details
CVE-2021-46634	This vulnerability allows remote attackers to execute arbitrary code on affected installations of Bentley MicroStation CONNECT 10.16.0.80. 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 JT files. Crafted data in a JT file can trigger 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-15464.	7.8	More Details
CVE-2021-44968	A Use after Free vulnerability exists in IOBit Advanced SystemCare 15 pro via requests sent in sequential order using the IOCTL driver codes, which could let a malicious user execute arbitrary code or a Denial of Service (system crash). IOCTL list: iobit_ioctl = [0x8001e01c, 0x8001e020, 0x8001e024, 0x8001e040,0x8001e044, 0x8001e048, 0x8001e04c, 0x8001e000, 0x8001e004, 0x8001e008, 0x8001e00c, 0x8001e010, 0x8001e014, 0x8001e018]	7.8	More Details
CVE-2021-46646	This vulnerability allows remote attackers to execute arbitrary code on affected installations of Bentley MicroStation CONNECT 10.16.0.80. 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 DGN files. Crafted data in a DGN file can trigger 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-15532.	7.8	More Details
CVE-2021-46648	This vulnerability allows remote attackers to execute arbitrary code on affected installations of Bentley MicroStation CONNECT 10.16.0.80. 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 DGN files. The issue results from the lack of proper validation of the length of user-supplied data prior to copying it to a heap-based buffer. An attacker can leverage this vulnerability to execute code in the context of the current process. Was ZDI-CAN-15534.	7.8	More Details
CVE-2021-46580	This vulnerability allows remote attackers to execute arbitrary code on affected installations of Bentley MicroStation CONNECT 10.16.0.80. 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 JT 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-15374.	7.8	More Details
CVE-2021-46641	This vulnerability allows remote attackers to execute arbitrary code on affected installations of Bentley View 10.15.0.75. 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 DGN file. Crafted data in a DNG file can trigger 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-15513.	7.8	More Details

CVE Number	Description	Base Score	Reference
CVE-2021-46562	This vulnerability allows remote attackers to execute arbitrary code on affected installations of Bentley MicroStation CONNECT 10.16.0.80. 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 JT files. Crafted data in a JT file can trigger 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-14987.	7.8	More Details
CVE-2021-46563	This vulnerability allows remote attackers to execute arbitrary code on affected installations of Bentley MicroStation CONNECT 10.16.0.80. 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 JT files. Crafted data in a JT file can trigger 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-14990.	7.8	More Details
CVE-2021-46564	This vulnerability allows remote attackers to execute arbitrary code on affected installations of Bentley MicroStation CONNECT 10.16.0.80. 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 JT files. Crafted data in a JT file can trigger 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-15023.	7.8	More Details
CVE-2021-46579	This vulnerability allows remote attackers to execute arbitrary code on affected installations of Bentley MicroStation CONNECT 10.16.0.80. 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 JT 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-15373.	7.8	More Details
CVE-2021-46584	This vulnerability allows remote attackers to execute arbitrary code on affected installations of Bentley MicroStation CONNECT 10.16.0.80. 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 J2K images. Crafted data in a J2K image can trigger 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-15378.	7.8	More Details
CVE-2021-46581	This vulnerability allows remote attackers to execute arbitrary code on affected installations of Bentley MicroStation CONNECT 10.16.0.80. 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 JT files. Crafted data in a JT file can trigger 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-15375.	7.8	More Details
CVE-2022-24057	This vulnerability allows remote attackers to execute arbitrary code on affected installations of Sante DICOM Viewer Pro 11.8.7.0. 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 J2K files. Crafted data in a J2K file can trigger 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-15077.	7.8	More Details

CVE Number	Description	Base Score	Reference
CVE-2021-46603	This vulnerability allows remote attackers to execute arbitrary code on affected installations of Bentley MicroStation CONNECT 10.16.0.80. 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 J2K images. The issue results from the lack of proper validation of the length of user-supplied data prior to copying it to a heap-based buffer. An attacker can leverage this vulnerability to execute code in the context of the current process. Was ZDI-CAN-15397.	7.8	More Details
CVE-2021-46604	This vulnerability allows remote attackers to execute arbitrary code on affected installations of Bentley MicroStation CONNECT 10.16.0.80. 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 PNG images. Crafted data in a PNG image can trigger 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-15398.	7.8	More Details
CVE-2021-46605	This vulnerability allows remote attackers to execute arbitrary code on affected installations of Bentley MicroStation CONNECT 10.16.0.80. 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 images. The issue results from the lack of proper validation of the length of user-supplied data prior to copying it to a heap-based buffer. An attacker can leverage this vulnerability to execute code in the context of the current process. Was ZDI-CAN-15399.	7.8	More Details
CVE-2021-46606	This vulnerability allows remote attackers to execute arbitrary code on affected installations of Bentley MicroStation CONNECT 10.16.0.80. 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 images. The issue results from the lack of proper validation of the length of user-supplied data prior to copying it to a heap-based buffer. An attacker can leverage this vulnerability to execute code in the context of the current process. Was ZDI-CAN-15400.	7.8	More Details
CVE-2022-24059	This vulnerability allows remote attackers to execute arbitrary code on affected installations of Sante DICOM Viewer Pro 11.8.7.0. 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 DCM files. Crafted data in a DCM file can trigger 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-15098.	7.8	More Details
CVE-2022-24058	This vulnerability allows remote attackers to execute arbitrary code on affected installations of Sante DICOM Viewer Pro 11.8.7.0. 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 J2K files. Crafted data in a J2K file can trigger 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-15095.	7.8	More Details
CVE-2021-46621	This vulnerability allows remote attackers to execute arbitrary code on affected installations of Bentley MicroStation CONNECT 10.16.0.80. 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 handling of JT files. The issue results from the lack of validating the existence of an object prior to performing further free operations on the object. An attacker can leverage this vulnerability to execute code in the context of the current process. Was ZDI-CAN-15415.	7.8	More Details

CVE Number	Description	Base Score	Reference
CVE-2021-46609	This vulnerability allows remote attackers to execute arbitrary code on affected installations of Bentley MicroStation CONNECT 10.16.0.80. 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 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-15403.	7.8	More Details
CVE-2022-24056	This vulnerability allows remote attackers to execute arbitrary code on affected installations of Sante DICOM Viewer Pro 11.8.7.0. 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 J2K files. Crafted data in a J2K file can trigger 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-15076.	7.8	More Details
CVE-2021-46582	This vulnerability allows remote attackers to execute arbitrary code on affected installations of Bentley MicroStation CONNECT 10.16.0.80. 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 JP2 images. 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-15376.	7.8	More Details
CVE-2021-46612	This vulnerability allows remote attackers to execute arbitrary code on affected installations of Bentley MicroStation CONNECT 10.16.0.80. 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. Crafted data in a PDF file can trigger 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-15406.	7.8	More Details
CVE-2021-46613	This vulnerability allows remote attackers to execute arbitrary code on affected installations of Bentley MicroStation CONNECT 10.16.0.80. 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 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-15407.	7.8	More Details
CVE-2021-46614	Bentley MicroStation CONNECT 10.16.0.80 J2K File Parsing Out-Of-Bounds Read Remote Code Execution Vulnerability. This vulnerability allows remote attackers to execute arbitrary code on affected installations of Bentley MicroStation CONNECT. 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 J2K images. Crafted data in a J2K image can trigger 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-15408.	7.8	More Details

CVE Number	Description	Base Score	Reference
CVE-2022-24052	MariaDB CONNECT Storage Engine Heap-based Buffer Overflow Privilege Escalation Vulnerability. This vulnerability allows local attackers to escalate privileges on affected installations of MariaDB. Authentication is required to exploit this vulnerability. The specific flaw exists within the processing of SQL queries. The issue results from the lack of proper validation of the length of user-supplied data prior to copying it to a fixed-length heap-based buffer. An attacker can leverage this vulnerability to escalate privileges and execute arbitrary code in the context of the service account. Was ZDI-CAN-16190.	7.8	More Details
CVE-2022-24051	MariaDB CONNECT Storage Engine Format String Privilege Escalation Vulnerability. This vulnerability allows local attackers to escalate privileges on affected installations of MariaDB. Authentication is required to exploit this vulnerability. The specific flaw exists within the processing of SQL queries. The issue results from the lack of proper validation of a user-supplied string before using it as a format specifier. An attacker can leverage this vulnerability to escalate privileges and execute arbitrary code in the context of the service account. Was ZDI-CAN-16193.	7.8	More Details
CVE-2021-46617	This vulnerability allows remote attackers to execute arbitrary code on affected installations of Bentley MicroStation CONNECT 10.16.0.80. 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 images. The issue results from the lack of proper initialization of memory prior to accessing it. An attacker can leverage this vulnerability to execute code in the context of the current process. Was ZDI-CAN-15411.	7.8	More Details
CVE-2022-24048	MariaDB CONNECT Storage Engine Stack-based Buffer Overflow Privilege Escalation Vulnerability. This vulnerability allows local attackers to escalate privileges on affected installations of MariaDB. Authentication is required to exploit this vulnerability. The specific flaw exists within the processing of SQL queries. The issue results from the lack of proper validation of the length of user-supplied data prior to copying it to a fixed-length stack-based buffer. An attacker can leverage this vulnerability to escalate privileges and execute arbitrary code in the context of the service account. Was ZDI-CAN-16191.	7.8	More Details
CVE-2022-24050	MariaDB CONNECT Storage Engine Use-After-Free Privilege Escalation Vulnerability. This vulnerability allows local attackers to escalate privileges on affected installations of MariaDB. Authentication is required to exploit this vulnerability. The specific flaw exists within the processing of SQL queries. 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 escalate privileges and execute arbitrary code in the context of the service account. Was ZDI-CAN-16207.	7.8	More Details
CVE-2021-46601	This vulnerability allows remote attackers to execute arbitrary code on affected installations of Bentley MicroStation CONNECT 10.16.0.80. 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 JT 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-15395.	7.8	More Details

CVE Number	Description	Base Score	Reference
CVE-2022-24062	This vulnerability allows remote attackers to execute arbitrary code on affected installations of Sante DICOM Viewer Pro 13.2.0.21165. 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 JP2 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-15104.	7.8	More Details
CVE-2022-24063	This vulnerability allows remote attackers to execute arbitrary code on affected installations of Sante DICOM Viewer Pro 13.2.0.21165. 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 JP2 files. The issue results from the lack of proper validation of user-supplied data, which can result in a memory corruption condition. An attacker can leverage this vulnerability to execute code in the context of the current process. Was ZDI-CAN-15105.	7.8	More Details
CVE-2021-46598	This vulnerability allows remote attackers to execute arbitrary code on affected installations of Bentley MicroStation CONNECT 10.16.0.80. 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 JT files. The issue results from the lack of proper validation of user-supplied data, which can result in a memory corruption condition. An attacker can leverage this vulnerability to execute code in the context of the current process. Was ZDI-CAN-15392.	7.8	More Details
CVE-2021-46583	This vulnerability allows remote attackers to execute arbitrary code on affected installations of Bentley MicroStation CONNECT 10.16.0.80. 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 J2K images. Crafted data in a J2K image can trigger 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-15377.	7.8	More Details
CVE-2021-46619	This vulnerability allows remote attackers to execute arbitrary code on affected installations of Bentley MicroStation CONNECT 10.16.0.80. 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. Crafted data in a PDF file can trigger 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-15413.	7.8	More Details
CVE-2021-46585	This vulnerability allows remote attackers to execute arbitrary code on affected installations of Bentley MicroStation CONNECT 10.16.0.80. 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 JT 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-15379.	7.8	More Details
CVE-2021-46586	This vulnerability allows remote attackers to execute arbitrary code on affected installations of Bentley MicroStation CONNECT 10.16.0.80. 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 3DS files. Crafted data in a 3DS file can trigger 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-15380.	7.8	More Details

CVE Number	Description	Base Score	Reference
CVE-2021-46587	This vulnerability allows remote attackers to execute arbitrary code on affected installations of Bentley MicroStation CONNECT 10.16.0.80. 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 3DS 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-15381.	7.8	More Details
CVE-2021-46588	This vulnerability allows remote attackers to execute arbitrary code on affected installations of Bentley MicroStation CONNECT 10.16.0.80. 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 JT 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-15382.	7.8	More Details
CVE-2021-46653	This vulnerability allows remote attackers to execute arbitrary code on affected installations of Bentley View 10.15.0.75. 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 images. The issue results from the lack of proper validation of the length of user-supplied data prior to copying it to a heap-based buffer. An attacker can leverage this vulnerability to execute code in the context of the current process. Was ZDI-CAN-15539.	7.8	More Details
CVE-2021-46655	This vulnerability allows remote attackers to execute arbitrary code on affected installations of Bentley View 10.15.0.75. 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 JT 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-15630.	7.8	More Details
CVE-2021-46590	This vulnerability allows remote attackers to execute arbitrary code on affected installations of Bentley MicroStation CONNECT 10.16.0.80. 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 JT files. Crafted data in a JT file can trigger 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-15384.	7.8	More Details
CVE-2021-46591	This vulnerability allows remote attackers to execute arbitrary code on affected installations of Bentley MicroStation CONNECT 10.16.0.80. 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 JT files. Crafted data in a JT file can trigger 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-15385.	7.8	More Details

CVE Number	Description	Base Score	Reference
CVE-2021-46592	This vulnerability allows remote attackers to execute arbitrary code on affected installations of Bentley MicroStation CONNECT 10.16.0.80. 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 3DS 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-15386.	7.8	More Details
CVE-2021-46627	This vulnerability allows remote attackers to execute arbitrary code on affected installations of Bentley View 10.15.0.75. 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 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-15457.	7.8	More Details
CVE-2021-46626	This vulnerability allows remote attackers to execute arbitrary code on affected installations of Bentley View 10.15.0.75. 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 J2K images. Crafted data in a J2K image can trigger 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-15456.	7.8	More Details
CVE-2021-46625	This vulnerability allows remote attackers to execute arbitrary code on affected installations of Bentley View 10.15.0.75. 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 handling of JT files. The issue results from the lack of validating the existence of an object prior to performing further free operations on the object. An attacker can leverage this vulnerability to execute code in the context of the current process. Was ZDI-CAN-15455.	7.8	More Details
CVE-2021-46656	This vulnerability allows remote attackers to execute arbitrary code on affected installations of Bentley View 10.15.0.75. 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 JT files. Crafted data in a JT file can trigger 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-15631.	7.8	More Details
CVE-2021-46622	This vulnerability allows remote attackers to execute arbitrary code on affected installations of Bentley MicroStation CONNECT 10.16.0.80. 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 J2K images. Crafted data in a J2K image can trigger 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-15416.	7.8	More Details
CVE-2021-46597	This vulnerability allows remote attackers to execute arbitrary code on affected installations of Bentley MicroStation CONNECT 10.16.0.80. 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 JT 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-15391.	7.8	More Details

CVE Number	Description	Base Score	Reference
CVE-2022-24064	This vulnerability allows remote attackers to execute arbitrary code on affected installations of Sante DICOM Viewer Pro 11.8.8.0. 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 J2K images. Crafted data in a J2K file can trigger 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-15161.	7.8	More Details
CVE-2021-46644	This vulnerability allows remote attackers to execute arbitrary code on affected installations of Bentley MicroStation CONNECT 10.16.0.80. 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 DGN files. Crafted data in a DGN file can trigger 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-15530.	7.8	More Details
CVE-2021-44730	snapd 2.54.2 did not properly validate the location of the snap-confine binary. A local attacker who can hardlink this binary to another location to cause snap-confine to execute other arbitrary binaries and hence gain privilege escalation. Fixed in snapd versions 2.54.3+18.04, 2.54.3+20.04 and 2.54.3+21.10.1	7.8	More Details
CVE-2021-22042	VMware ESXi contains an unauthorized access vulnerability due to VMX having access to settingsd authorization tickets. A malicious actor with privileges within the VMX process only, may be able to access settingsd service running as a high privileged user.	7.8	More Details
CVE-2021-44731	A race condition existed in the snapd 2.54.2 snap-confine binary when preparing a private mount namespace for a snap. This could allow a local attacker to gain root privileges by bind-mounting their own contents inside the snap's private mount namespace and causing snap-confine to execute arbitrary code and hence gain privilege escalation. Fixed in snapd versions 2.54.3+18.04, 2.54.3+20.04 and 2.54.3+21.10.1	7.8	More Details
CVE-2022-23803	A stack-based buffer overflow vulnerability exists in the Gerber Viewer gerber and excellon ReadXYCoord coordinate parsing functionality of KiCad EDA 6.0.1 and master commit de006fc010. A specially-crafted gerber or excellon file can lead to code execution. An attacker can provide a malicious file to trigger this vulnerability.	7.8	More Details
CVE-2022-25366	Cryptomator through 1.6.5 allows DYLIB injection because, although it has the flag 0x1000 for Hardened Runtime, it has the com.apple.security.cs.disable-library-validation and com.apple.security.cs.allow-dyld-environment-variables entitlements. An attacker can exploit this by creating a malicious .dylib file that can be executed via the DYLD_INSERT_LIBRARIES environment variable.	7.8	More Details
CVE-2022-0409	Unrestricted Upload of File with Dangerous Type in Packagist showdoc/showdoc prior to 2.10.2.	7.8	More Details
CVE-2021-3551	A flaw was found in the PKI-server, where the spkispawn command, when run in debug mode, stores admin credentials in the installation log file. This flaw allows a local attacker to retrieve the file to obtain the admin password and gain admin privileges to the Dogtag CA manager. The highest threat from this vulnerability is to confidentiality.	7.8	More Details
CVE-2021-4106	A vulnerability in Snow Inventory Java Scanner allows an attacker to run malicious code at a higher level of privileges. This issue affects: SNOW Snow Inventory Java Scanner 1.0	7.8	More Details

CVE Number	Description	Base Score	Reference
CVE-2022-0685	Use of Out-of-range Pointer Offset in GitHub repository vim/vim prior to 8.2.4418.	7.8	More Details
CVE-2022-22945	VMware NSX Edge contains a CLI shell injection vulnerability. A malicious actor with SSH access to an NSX-Edge appliance can execute arbitrary commands on the operating system as root.	7.8	More Details
CVE-2022-23186	Adobe Illustrator versions 25.4.3 (and earlier) and 26.0.2 (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-2022-0629	Stack-based Buffer Overflow in GitHub repository vim/vim prior to 8.2.	7.8	More Details
CVE-2021-46368	TRIGONE Remote System Monitor 3.61 is vulnerable to an unquoted path service allowing local users to launch processes with elevated privileges.	7.8	More Details
CVE-2022-23188	Adobe Illustrator versions 25.4.3 (and earlier) and 26.0.2 (and earlier) are affected by a buffer overflow vulnerability due to insecure handling of a crafted malicious file, potentially resulting in arbitrary code execution in the context of the current user. Exploitation requires user interaction in that a victim must open a crafted malicious file in Illustrator.	7.8	More Details
CVE-2022-25372	Pritunl Client through 1.2.3019.52 on Windows allows local privilege escalation, related to an ACL entry for CREATOR OWNER in platform_windows.go.	7.8	More Details
CVE-2021-46699	A vulnerability has been identified in Simcenter Femap (All versions < V2022.1.1). Affected application contains a stack based buffer overflow vulnerability while parsing specially crafted BDF files. This could allow an attacker to execute code in the context of the current process. (ZDI-CAN-15061)	7.8	More Details
CVE-2021-46162	A vulnerability has been identified in Simcenter Femap (All versions < V2022.1.1). Affected application contains an out of bounds write past the end of an allocated structure while parsing specially crafted NEU files. This could allow an attacker to execute code in the context of the current process. (ZDI-CAN-15048)	7.8	More Details
CVE-2022-0676	Heap-based Buffer Overflow in GitHub repository radareorg/radare2 prior to 5.6.4.	7.8	More Details
CVE-2022-25265	In the Linux kernel through 5.16.10, certain binary files may have the exec-all attribute if they were built in approximately 2003 (e.g., with GCC 3.2.2 and Linux kernel 2.4.20). This can cause execution of bytes located in supposedly non-executable regions of a file.	7.8	More Details
CVE-2022-25255	In Qt 5.9.x through 5.15.x before 5.15.9 and 6.x before 6.2.4 on Linux and UNIX, QProcess could execute a binary from the current working directory when not found in the PATH.	7.8	More Details

CVE Number	Description	Base Score	Reference
CVE-2021-3760	A flaw was found in the Linux kernel. A use-after-free vulnerability in the NFC stack can lead to a threat to confidentiality, integrity, and system availability.	7.8	More Details
CVE-2022-22308	IBM Planning Analytics 2.0 is vulnerable to a Remote File Include (RFI) attack. User input could be passed into file include commands and the web application could be tricked into including remote files with malicious code. IBM X-Force ID: 216891.	7.8	More Details
CVE-2022-23203	Adobe Photoshop versions 22.5.4 (and earlier) and 23.1 (and earlier) are affected by a buffer overflow vulnerability due to insecure handling of a crafted file, potentially resulting in arbitrary code execution in the context of the current user. Exploitation requires user interaction in that a victim must open a crafted file in Photoshop.	7.8	More Details
CVE-2021-3578	A flaw was found in mbsync before v1.3.6 and v1.4.2, where an unchecked pointer cast allows a malicious or compromised server to write an arbitrary integer value past the end of a heap-allocated structure by issuing an unexpected APPENDUID response. This could be plausibly exploited for remote code execution on the client.	7.8	More Details
CVE-2021-3560	It was found that polkit could be tricked into bypassing the credential checks for D-Bus requests, elevating the privileges of the requestor to the root user. This flaw could be used by an unprivileged local attacker to, for example, create a new local administrator. The highest threat from this vulnerability is to data confidentiality and integrity as well as system availability.	7.8	More Details
CVE-2022-25365	Docker Desktop before 4.5.1 on Windows allows attackers to move arbitrary files. NOTE: this issue exists because of an incomplete fix for CVE-2022-23774.	7.8	More Details
CVE-2022-23804	A stack-based buffer overflow vulnerability exists in the Gerber Viewer gerber and excellon ReadIJCoord coordinate parsing functionality of KiCad EDA 6.0.1 and master commit de006fc010. A specially-crafted gerber or excellon file can lead to code execution. An attacker can provide a malicious file to trigger this vulnerability.	7.8	More Details
CVE-2021-46645	This vulnerability allows remote attackers to execute arbitrary code on affected installations of Bentley MicroStation CONNECT 10.16.0.80. 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 images. Crafted data in a BMP image can trigger 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-15531.	7.8	More Details
CVE-2020-6917	Potential security vulnerabilities including compromise of integrity, and allowed communication with untrusted clients has been identified in HP Support Assistant software.	7.8	More Details
CVE-2020-6922	Potential security vulnerabilities including compromise of integrity, and allowed communication with untrusted clients has been identified in HP Support Assistant software.	7.8	More Details
CVE-2020-6919	Potential security vulnerabilities including compromise of integrity, and allowed communication with untrusted clients has been identified in HP Support Assistant software.	7.8	More Details

CVE Number	Description	Base Score	Reference
CVE-2021-45082	An issue was discovered in Cobbler before 3.3.1. In the templar.py file, the function check_for_invalid_imports can allow Cheetah code to import Python modules via the "#from MODULE import" substring. (Only lines beginning with #import are blocked.)	7.8	More Details
CVE-2020-6918	Potential security vulnerabilities including compromise of integrity, and allowed communication with untrusted clients has been identified in HP Support Assistant software.	7.8	More Details
CVE-2020-6921	Potential security vulnerabilities including compromise of integrity, and allowed communication with untrusted clients has been identified in HP Support Assistant software.	7.8	More Details
CVE-2021-21958	A heap-based buffer overflow vulnerability exists in the Hword HwordApp.dll functionality of Hancom Office 2020 11.0.0.2353. A specially-crafted malformed file can lead to memory corruption and potential arbitrary code execution. An attacker can provide a malicious file to trigger this vulnerability.	7.8	More Details
CVE-2021-23702	The package object-extend from 0.0.0 are vulnerable to Prototype Pollution via object-extend.	7.6	More Details
CVE-2022-25297	This affects the package drogonframework/drogon before 1.7.5. The unsafe handling of file names during upload using HttpFile::save() method may enable attackers to write files to arbitrary locations outside the designated target folder.	7.5	More Details
CVE-2021-43826	Envoy is an open source edge and service proxy, designed for cloud-native applications. In affected versions of Envoy a crash occurs when configured for :ref:`upstream tunneling <envoy_v3_api_field_extensions.filters.network.tcp_proxy.v3.TcpProxy.tunneling_config>` and the downstream connection disconnects while the the upstream connection or http/2 stream is still being established. There are no workarounds for this issue. Users are advised to upgrade.	7.5	More Details
CVE-2022-24983	Forms generated by JQueryForm.com before 2022-02-05 allow remote attackers to obtain the URI to any uploaded file by capturing the POST response. When chained with CVE-2022-24984, this could lead to unauthenticated remote code execution on the underlying web server. This occurs because the Unique ID field is contained in the POST response upon submitting a form.	7.5	More Details
CVE-2022-25271	Drupal core's form API has a vulnerability where certain contributed or custom modules' forms may be vulnerable to improper input validation. This could allow an attacker to inject disallowed values or overwrite data. Affected forms are uncommon, but in certain cases an attacker could alter critical or sensitive data.	7.5	More Details
CVE-2021-45391	A Buffer Overflow vulnerability exists in Tenda Router AX12 V22.03.01.21_CN in the sub_422CE4 function in the goform/setIPv6Status binary file /usr/sbin/httpd via the conType parameter, which causes a Denial of Service.	7.5	More Details
CVE-2021-4091	A double-free was found in the way 389-ds-base handles virtual attributes context in persistent searches. An attacker could send a series of search requests, forcing the server to behave unexpectedly, and crash.	7.5	More Details

CVE Number	Description	Base Score	Reference
CVE-2021-38935	IBM Maximo Asset Management 7.6.1.2 does not require that users should have strong passwords by default, which makes it easier for attackers to compromise user accounts. IBM X-Force ID: 210892.	7.5	More Details
CVE-2022-0138	MMP: All versions prior to v1.0.3, PTP C-series: Device versions prior to v2.8.6.1, and PTMP C-series and A5x: Device versions prior to v2.5.4.1 has a deserialization function that does not validate or check the data, allowing arbitrary classes to be created.	7.5	More Details
CVE-2022-23647	Prism is a syntax highlighting library. Starting with version 1.14.0 and prior to version 1.27.0, Prism's command line plugin can be used by attackers to achieve a cross-site scripting attack. The command line plugin did not properly escape its output, leading to the input text being inserted into the DOM as HTML code. Server-side usage of Prism is not impacted. Websites that do not use the Command Line plugin are also not impacted. This bug has been fixed in v1.27.0. As a workaround, do not use the command line plugin on untrusted inputs, or sanitize all code blocks (remove all HTML code text) from all code blocks that use the command line plugin.	7.5	More Details
CVE-2022-21655	Envoy is an open source edge and service proxy, designed for cloud-native applications. The envoy common router will segfault if an internal redirect selects a route configured with direct response or redirect actions. This will result in a denial of service. As a workaround turn off internal redirects if direct response entries are configured on the same listener.	7.5	More Details
CVE-2022-0666	CRLF Injection leads to Stack Trace Exposure due to lack of filtering at https://demo.microweber.org/ in Packagist microweber/microweber prior to 1.2.11.	7.5	More Details
CVE-2021-43824	Envoy is an open source edge and service proxy, designed for cloud-native applications. In affected versions a crafted request crashes Envoy when a CONNECT request is sent to JWT filter configured with regex match. This provides a denial of service attack vector. The only workaround is to not use regex in the JWT filter. Users are advised to upgrade.	7.5	More Details
CVE-2022-21143	MMP: All versions prior to v1.0.3, PTP C-series: Device versions prior to v2.8.6.1, and PTMP C-series and A5x: Device versions prior to v2.5.4.1 does not properly sanitize user input on several locations, which may allow an attacker to inject arbitrary commands.	7.5	More Details
CVE-2022-23635	Istio is an open platform to connect, manage, and secure microservices. In affected versions the Istio control plane, `istiod`, is vulnerable to a request processing error, allowing a malicious attacker that sends a specially crafted message which results in the control plane crashing. This endpoint is served over TLS port 15012, but does not require any authentication from the attacker. For simple installations, Istiod is typically only reachable from within the cluster, limiting the blast radius. However, for some deployments, especially [multicluster] (https://istio.io/latest/docs/setup/install/multicluster/primary-remote/) topologies, this port is exposed over the public internet. There are no effective workarounds, beyond upgrading. Limiting network access to Istiod to the minimal set of clients can help lessen the scope of the vulnerability to some extent.	7.5	More Details
CVE-2016-20013	sha256crypt and sha512crypt through 0.6 allow attackers to cause a denial of service (CPU consumption) because the algorithm's runtime is proportional to the square of the length of the password.	7.5	More Details

CVE Number	Description	Base Score	Reference
CVE-2021-46082	Moxa TN-5900 v3.1 series routers, MGate 5109 v2.2 series protocol gateways, and MGate 5101-PBM-MN v2.1 series protocol gateways were discovered to contain a memory leak which allows attackers to cause a Denial of Service (DoS) via crafted packets.	7.5	More Details
CVE-2022-25314	In Expat (aka libexpat) before 2.4.5, there is an integer overflow in copyString.	7.5	More Details
CVE-2017-0371	MediaWiki before 1.23.16, 1.24.x through 1.27.x before 1.27.2, and 1.28.x before 1.28.1 allows remote attackers to discover the IP addresses of Wiki visitors via a style="background-image: attr(title url);" attack within a DIV element that has an attacker-controlled URL in the title attribute.	7.5	More Details
CVE-2022-25335	RigoBlock Dragos through 2022-02-17 lacks the onlyOwner modifier for setMultipleAllowances. This enables token manipulation, as exploited in the wild in February 2022. NOTE: although 2022-02-17 is the vendor's vulnerability announcement date, the vulnerability will not be remediated until a major protocol upgrade occurs.	7.5	More Details
CVE-2022-0660	Generation of Error Message Containing Sensitive Information in Packagist microweber/microweber prior to 1.2.11.	7.5	More Details
CVE-2022-24980	An issue was discovered in the Kitodo.Presentation (aka dif) extension before 2.3.2, 3.x before 3.2.3, and 3.3.x before 3.3.4 for TYPO3. A missing access check in an eID script allows an unauthenticated user to submit arbitrary URLs to this component. This results in SSRF, allowing attackers to view the content of any file or webpage the webserver has access to.	7.5	More Details
CVE-2022-20653	A vulnerability in the DNS-based Authentication of Named Entities (DANE) email verification component of Cisco AsyncOS Software for Cisco Email Security Appliance (ESA) could allow an unauthenticated, remote attacker to cause a denial of service (DoS) condition on an affected device. This vulnerability is due to insufficient error handling in DNS name resolution by the affected software. An attacker could exploit this vulnerability by sending specially formatted email messages that are processed by an affected device. A successful exploit could allow the attacker to cause the device to become unreachable from management interfaces or to process additional email messages for a period of time until the device recovers, resulting in a DoS condition. Continued attacks could cause the device to become completely unavailable, resulting in a persistent DoS condition.	7.5	More Details
CVE-2022-22914	An incorrect access control issue in the component FileManager of Ovidentia CMS 6.0 allows authenticated attackers to to view and download content in the upload directory via path traversal.	7.5	More Details
CVE-2021-22043	VMware ESXi contains a TOCTOU (Time-of-check Time-of-use) vulnerability that exists in the way temporary files are handled. A malicious actor with access to settingsd, may exploit this issue to escalate their privileges by writing arbitrary files.	7.5	More Details
CVE-2021-46247	The use of a hard-coded cryptographic key significantly increases the possibility encrypted data may be recovered from ASUS CMAX6000 v1.02.00.	7.5	More Details

CVE Number	Description	Base Score	Reference
CVE-2022-23228	Pexip Infinity before 27.0 has improper WebRTC input validation. An unauthenticated remote attacker can use excessive resources, temporarily causing denial of service.	7.5	More Details
CVE-2022-24683	HashiCorp Nomad and Nomad Enterprise 0.9.2 through 1.0.17, 1.1.11, and 1.2.5 allow operators with read-fs and alloc-exec (or job-submit) capabilities to read arbitrary files on the host filesystem as root.	7.5	More Details
CVE-2021-22050	ESXi contains a slow HTTP POST denial-of-service vulnerability in rhttpproxy. A malicious actor with network access to ESXi may exploit this issue to create a denial-of-service condition by overwhelming rhttpproxy service with multiple requests.	7.5	More Details
CVE-2021-39034	IBM MQ 9.1 LTS is vulnerable to a denial of service attack caused by an issue within the channel process. IBM X-Force ID: 213964.	7.5	More Details
CVE-2022-25298	This affects the package sprinfall/webcc before 0.3.0. It is possible to traverse directories to fetch arbitrary files from the server.	7.5	More Details
CVE-2022-23612	OpenMRS is a patient-based medical record system focusing on giving providers a free customizable electronic medical record system. Affected versions are subject to arbitrary file exfiltration due to failure to sanitize request when satisfying GET requests for `/images` & `/initfilter/scripts`. This can allow an attacker to access any file on a system running OpenMRS that is accessible to the user id OpenMRS is running under. Affected implementations should update to the latest patch version of OpenMRS Core for the minor version they use. These are: 2.1.5, 2.2.1, 2.3.5, 2.4.5 and 2.5.3. As a general rule, this vulnerability is already mitigated by Tomcat's URL normalization in Tomcat 7.0.28+. Users on older versions of Tomcat should consider upgrading their Tomcat instance as well as their OpenMRS instance.	7.5	More Details
CVE-2022-21654	Envoy is an open source edge and service proxy, designed for cloud-native applications. Envoy's tls allows re-use when some cert validation settings have changed from their default configuration. The only workaround for this issue is to ensure that default tls settings are used. Users are advised to upgrade.	7.4	More Details
CVE-2022-21656	Envoy is an open source edge and service proxy, designed for cloud-native applications. The default_validator.cc implementation used to implement the default certificate validation routines has a "type confusion" bug when processing subjectAltNames. This processing allows, for example, an rfc822Name or uniformResourceIndicator to be authenticated as a domain name. This confusion allows for the bypassing of nameConstraints, as processed by the underlying OpenSSL/BoringSSL implementation, exposing the possibility of impersonation of arbitrary servers. As a result Envoy will trust upstream certificates that should not be trusted.	7.4	More Details
CVE-2021-20322	A flaw in the processing of received ICMP errors (ICMP fragment needed and ICMP redirect) in the Linux kernel functionality was found to allow the ability to quickly scan open UDP ports. This flaw allows an off-path remote user to effectively bypass the source port UDP randomization. The highest threat from this vulnerability is to confidentiality and possibly integrity, because software that relies on UDP source port randomization are indirectly affected as well.	7.4	More Details

CVE Number	Description	Base Score	Reference
CVE-2022-23632	Traefik is an HTTP reverse proxy and load balancer. Prior to version 2.6.1, Traefik skips the router transport layer security (TLS) configuration when the host header is a fully qualified domain name (FQDN). For a request, the TLS configuration choice can be different than the router choice, which implies the use of a wrong TLS configuration. When sending a request using FQDN handled by a router configured with a dedicated TLS configuration, the TLS configuration falls back to the default configuration that might not correspond to the configured one. If the CNAME flattening is enabled, the selected TLS configuration is the SNI one and the routing uses the CNAME value, so this can skip the expected TLS configuration. Version 2.6.1 contains a patch for this issue. As a workaround, one may add the FDQN to the host rule. However, there is no workaround if the CNAME flattening is enabled.	7.4	More Details
CVE-2021-23682	This affects the package litespeed.js before 0.3.12; the package appwrite/server-ce from 0.12.0 and before 0.12.2, before 0.11.1. When parsing the query string in the getJsonFromUrl function, the key that is set in the result object is not properly sanitized leading to a Prototype Pollution vulnerability.	7.3	More Details
CVE-2022-0228	The Popup Builder WordPress plugin before 4.0.7 does not validate and properly escape the orderby and order parameters before using them in a SQL statement in the admin dashboard, which could allow high privilege users to perform SQL injection	7.2	More Details
CVE-2021-4134	The Fancy Product Designer WordPress plugin is vulnerable to SQL Injection due to insufficient escaping and parameterization of the ID parameter found in the ~/inc/api/class-view.php file which allows attackers with administrative level permissions to inject arbitrary SQL queries to obtain sensitive information, in versions up to and including 4.7.4.	7.2	More Details
CVE-2022-0255	The Database Backup for WordPress plugin before 2.5.1 does not properly sanitise and escape the fragment parameter before using it in a SQL statement in the admin dashboard, leading to a SQL injection issue	7.2	More Details
CVE-2020-8242	Unsanitized user input in ExpressionEngine <= 5.4.0 control panel member creation leads to an SQL injection. The user needs member creation/admin control panel access to execute the attack.	7.2	More Details
CVE-2020-25719	A flaw was found in the way Samba, as an Active Directory Domain Controller, implemented Kerberos name-based authentication. The Samba AD DC, could become confused about the user a ticket represents if it did not strictly require a Kerberos PAC and always use the SIDs found within. The result could include total domain compromise.	7.2	More Details
CVE-2021-4208	The ExportFeed WordPress plugin through 2.0.1.0 does not sanitise and escape the product_id POST parameter before using it in a SQL statement, leading to a SQL injection vulnerability exploitable by high privilege users	7.2	More Details
CVE-2022-23650	Netmaker is a platform for creating and managing virtual overlay networks using WireGuard. Prior to versions 0.8.5, 0.9.4, and 010.0, there is a hard-coded cryptographic key in the code base which can be exploited to run admin commands on a remote server if the exploiter know the address and username of the admin. This effects the server (netmaker) component, and not clients. This has been patched in Netmaker v0.8.5, v0.9.4, and v0.10.0. There are currently no known workarounds.	7.2	More Details
CVE-2021-46701	PreMiD 2.2.0 allows unintended access via the websocket transport. An attacker can receive events from a socket and emit events to a socket, potentially interfering with a victim's "now playing" status on Discord.	7.2	More Details

CVE Number	Description	Base Score	Reference
CVE-2021-26619	An path traversal vulnerability leading to delete arbitrary files was discovered in BigFileAgent. Remote attackers can use this vulnerability to delete arbitrary files of unspecified number of users.	7.1	More Details
CVE-2021-4090	An out-of-bounds (OOB) memory write flaw was found in the NFSD in the Linux kernel. Missing sanity may lead to a write beyond bmval[bmlen-1] in nfsd4_decode_bitmap4 in fs/nfsd/nfs4xdr.c. In this flaw, a local attacker with user privilege may gain access to out-of-bounds memory, leading to a system integrity and confidentiality threat.	7.1	More Details
CVE-2021-46062	MCMS v5.2.5 was discovered to contain an arbitrary file deletion vulnerability via the component oldFileName.	7.1	More Details
CVE-2021-3752	A use-after-free flaw was found in the Linux kernel's Bluetooth subsystem in the way user calls connect to the socket and disconnect simultaneously due to a race condition. This flaw allows a user to crash the system or escalate their privileges. The highest threat from this vulnerability is to confidentiality, integrity, as well as system availability.	7.1	More Details
CVE-2022-0630	Out-of-bounds Read in Homebrew mruby prior to 3.2.	7.1	More Details
CVE-2021-45083	An issue was discovered in Cobbler before 3.3.1. Files in /etc/cobbler are world readable. Two of those files contain some sensitive information that can be exposed to a local user who has non-privileged access to the server. The users.digest file contains the sha2-512 digest of users in a Cobbler local installation. In the case of an easy-to-guess password, it's trivial to obtain the plaintext string. The settings.yaml file contains secrets such as the hashed default password.	7.1	More Details
CVE-2022-0713	Heap-based Buffer Overflow in GitHub repository radareorg/radare2 prior to 5.6.4.	7.1	More Details
CVE-2022-23318	A heap-buffer-overflow in pcf2bdf, versions >= 1.05 allows an attacker to trigger unsafe memory access via a specially crafted PCF font file. This out-of-bound read may lead to an application crash, information disclosure via program memory or other context-dependent impact.	7.1	More Details
CVE-2021-26618	An improper input validation leading to arbitrary file creation was discovered in ToWord of ToOffice. Remote attackers use this vulnerability to execute arbitrary file included malicious code.	7.1	More Details
CVE-2022-23202	Adobe Creative Cloud Desktop version 2.7.0.13 (and earlier) is affected by an Uncontrolled Search Path Element 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 download a malicious DLL file. The attacker has to deliver the DLL on the same folder as the installer which makes it as a high complexity attack vector.	7.0	More Details

CVE Number	Description	Base Score	Reference
CVE-2022-21657	Envoy is an open source edge and service proxy, designed for cloud-native applications. In affected versions Envoy does not restrict the set of certificates it accepts from the peer, either as a TLS client or a TLS server, to only those certificates that contain the necessary extendedKeyUsage (id-kp-serverAuth and id-kp-clientAuth, respectively). This means that a peer may present an e-mail certificate (e.g. id-kp-emailProtection), either as a leaf certificate or as a CA in the chain, and it will be accepted for TLS. This is particularly bad when combined with the issue described in pull request #630, in that it allows a Web PKI CA that is intended only for use with S/MIME, and thus exempted from audit or supervision, to issue TLS certificates that will be accepted by Envoy. As a result Envoy will trust upstream certificates that should not be trusted. There are no known workarounds to this issue. Users are advised to upgrade.	6.8	More Details
CVE-2021-22041	VMware ESXi, Workstation, and Fusion contain a double-fetch vulnerability in the UHCI USB controller. A malicious actor with local administrative privileges on a virtual machine may exploit this issue to execute code as the virtual machine's VMX process running on the host.	6.7	More Details
CVE-2021-22040	VMware ESXi, Workstation, and Fusion contain a use-after-free vulnerability in the XHCI USB controller. A malicious actor with local administrative privileges on a virtual machine may exploit this issue to execute code as the virtual machine's VMX process running on the host.	6.7	More Details
CVE-2022-22792	MobiSoft - MobiPlus User Take Over and Improper Handling of url Parameters Attacker can navigate to specific url which will expose all the users and password in clear text. http://IP/MobiPlusWeb/Handlers/MainHandler.ashx?MethodName=GridData&GridName=Users	6.6	More Details
CVE-2019-4291	IBM Maximo Anywhere 7.6.4.0 could allow an attacker to reverse engineer the application due to the lack of binary protection precautions. IBM X-Force ID: 160697.	6.5	More Details
CVE-2021-27796	A vulnerability in Brocade Fabric OS versions before Brocade Fabric OS v8.0.1b, v7.4.1d could allow an authenticated attacker within the restricted shell environment (rbash) as either the “user” or “factory” account, to read the contents of any file on the filesystem utilizing one of a few available binaries.	6.5	More Details
CVE-2021-3930	An off-by-one error was found in the SCSI device emulation in QEMU. It could occur while processing MODE SELECT commands in mode_sense_page() if the 'page' argument was set to MODE_PAGE_ALLS (0x3f). A malicious guest could use this flaw to potentially crash QEMU, resulting in a denial of service condition.	6.5	More Details
CVE-2022-24370	This vulnerability allows remote attackers to disclose sensitive information on affected installations of Foxit PDF Reader Foxit reader 11.0.1.0719 macOS. 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 handling of XFA forms. 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 object. An attacker can leverage this in conjunction with other vulnerabilities to execute arbitrary code in the context of the current process. Was ZDI-CAN-14819.	6.5	More Details
CVE-2022-24982	Forms generated by JQueryForm.com before 2022-02-05 allows a remote authenticated attacker to access the cleartext credentials of all other form users. admin.php contains a hidden base64-encoded string with these credentials.	6.5	More Details

CVE Number	Description	Base Score	Reference
CVE-2022-24368	This vulnerability allows remote attackers to disclose sensitive information on affected installations of Foxit PDF Reader 11.1.0.52543. 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 handling of Doc objects. 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 in conjunction with other vulnerabilities to execute arbitrary code in the context of the current process. Was ZDI-CAN-16115.	6.5	More Details
CVE-2022-0613	Authorization Bypass Through User-Controlled Key in NPM urijs prior to 1.19.8.	6.5	More Details
CVE-2021-44568	Two heap-overflow vulnerabilities exist in openSUSE/libsolv libsolv through 13 Dec 2020 in the decisionmap variable via the resolve_dependencies function at src/solver.c (line 1940 & line 1995), which could cause a remote Denial of Service.	6.5	More Details
CVE-2022-0673	A flaw was found in LemMinX in versions prior to 0.19.0. Cache poisoning of external schema files due to directory traversal.	6.5	More Details
CVE-2021-40841	A Path Traversal vulnerability for a log file in LiveConfig 2.12.2 allows authenticated attackers to read files on the underlying server.	6.5	More Details
CVE-2022-0451	Dart SDK contains the HTTPClient in dart:io library whcih includes authorization headers when handling cross origin redirects. These headers may be explicitly set and contain sensitive information. By default, HttpClient handles redirection logic. If a request is sent to example.com with authorization header and it redirects to an attackers site, they might not expect attacker site to receive authorization header. We recommend updating the Dart SDK to version 2.16.0 or beyond.	6.5	More Details
CVE-2022-21800	MMP: All versions prior to v1.0.3, PTP C-series: Device versions prior to v2.8.6.1, and PTMP C-series and A5x: Device versions prior to v2.5.4.1 uses the MD5 algorithm to hash the passwords before storing them but does not salt the hash. As a result, attackers may be able to crack the hashed passwords.	6.5	More Details
CVE-2022-0665	Path Traversal in GitHub repository pimcore/pimcore prior to 10.3.2.	6.5	More Details
CVE-2022-25313	In Expat (aka libexpat) before 2.4.5, an attacker can trigger stack exhaustion in build_model via a large nesting depth in the DTD element.	6.5	More Details
CVE-2022-0633	The UpdraftPlus WordPress plugin Free before 1.22.3 and Premium before 2.22.3 do not properly validate a user has the required privileges to access a backup's nonce identifier, which may allow any users with an account on the site (such as subscriber) to download the most recent site & database backup.	6.5	More Details
CVE-2021-45007	Plesk 18.0.37 is affected by a Cross Site Request Forgery (CSRF) vulnerability that allows an attacker to insert data on the user and admin panel. NOTE: the vendor states that this is only a site-specific problem on websites of one or more Plesk users	6.5	More Details

CVE Number	Description	Base Score	Reference
CVE-2021-3557	A flaw was found in argocd. Any unprivileged user is able to deploy argocd in their namespace and with the created ServiceAccount argocd-argocd-server, the unprivileged user is able to read all resources of the cluster including all secrets which might enable privilege escalations. The highest threat from this vulnerability is to data confidentiality.	6.5	More Details
CVE-2021-46700	In libsixel 1.8.6, sixel_encoder_output_without_macro (called from sixel_encoder_encode_frame in encoder.c) has a double free.	6.5	More Details
CVE-2022-25270	The Quick Edit module does not properly check entity access in some circumstances. This could result in users with the "access in-place editing" permission viewing some content they are are not authorized to access. Sites are only affected if the QuickEdit module (which comes with the Standard profile) is installed.	6.5	More Details
CVE-2022-0611	Missing Authorization in Packagist snipe/snipe-it prior to 5.3.11.	6.3	More Details
CVE-2021-3948	An incorrect default permissions vulnerability was found in the mig-controller. Due to an incorrect cluster namespaces handling an attacker may be able to migrate a malicious workload to the target cluster, impacting confidentiality, integrity, and availability of the services located on that cluster.	6.3	More Details
CVE-2022-23645	swtpm is a libtpms-based TPM emulator with socket, character device, and Linux CUSE interface. Versions prior to 0.5.3, 0.6.2, and 0.7.1 are vulnerable to out-of-bounds read. A specially crafted header of swtpm's state, where the blobheader's hdrsize indicator has an invalid value, may cause an out-of-bounds access when the byte array representing the state of the TPM is accessed. This will likely crash swtpm or prevent it from starting since the state cannot be understood. Users should upgrade to swtpm v0.5.3, v0.6.2, or v0.7.1 to receive a patch. There are currently no known workarounds.	6.2	More Details
CVE-2022-23054	Openmct versions 1.3.0 to 1.7.7 are vulnerable against stored XSS via the “Summary Widget” element, that allows the injection of malicious JavaScript into the ‘URL’ field. This issue affects: nasa openmct 1.7.7 version and prior versions; 1.3.0 version and later versions.	6.1	More Details
CVE-2022-23053	Openmct versions 1.3.0 to 1.7.7 are vulnerable against stored XSS via the “Condition Widget” element, that allows the injection of malicious JavaScript into the ‘URL’ field. This issue affects: nasa openmct 1.7.7 version and prior versions; 1.3.0 version and later versions.	6.1	More Details
CVE-2022-0252	The GiveWP WordPress plugin before 2.17.3 does not escape the json parameter before outputting it back in an attribute in the Import admin dashboard, leading to a Reflected Cross-Site Scripting	6.1	More Details
CVE-2022-0234	The WOOCS WordPress plugin before 1.3.7.5 does not sanitise and escape the woocs_in_order_currency parameter of the woocs_get_products_price_html AJAX action (available to both unauthenticated and authenticated users) before outputting it back in the response, leading to a Reflected Cross-Site Scripting	6.1	More Details
CVE-2021-25100	The GiveWP WordPress plugin before 2.17.3 does not escape the s parameter before outputting it back in an attribute in the Donation Forms dashboard, leading to a Reflected Cross-Site Scripting	6.1	More Details

CVE Number	Description	Base Score	Reference
CVE-2021-25099	The GiveWP WordPress plugin before 2.17.3 does not sanitise and escape the form_id parameter before outputting it back in the response of an unauthenticated request via the give_checkout_login AJAX action, leading to a Reflected Cross-Site Scripting	6.1	More Details
CVE-2021-25055	The FeedWordPress plugin before 2022.0123 is affected by a Reflected Cross-Site Scripting (XSS) within the "visibility" parameter.	6.1	More Details
CVE-2021-24921	The Advanced Database Cleaner WordPress plugin before 3.0.4 does not sanitise and escape $_GET keys and values before outputting them back in attributes, leading to Reflected Cross-Site Scripting issues	6.1	More Details
CVE-2022-24981	A reflected cross-site scripting (XSS) vulnerability in forms generated by JQueryForm.com before 2022-02-05 allows remote attackers to inject arbitrary web script or HTML via the redirect parameter to admin.php.	6.1	More Details
CVE-2021-30650	A reflected cross-site scripting (XSS) vulnerability in the Symantec Layer7 API Management OAuth Toolkit (OTK) allows a remote attacker to craft a malicious URL for the OTK web UI and target OTK users with phishing attacks or other social engineering techniques. A successful attack allows injecting malicious code into the OTK web UI client application.	6.1	More Details
CVE-2021-20315	A locking protection bypass flaw was found in some versions of gnome-shell as shipped within CentOS Stream 8, when the "Application menu" or "Window list" GNOME extensions are enabled. This flaw allows a physical attacker who has access to a locked system to kill existing applications and start new ones as the locked user, even if the session is still locked.	6.1	More Details
CVE-2022-0692	Open Redirect on Rudloff/alltube in Packagist rudloff/alltube prior to 3.0.1.	6.1	More Details
CVE-2022-22126	Openmct versions 1.3.0 to 1.7.7 are vulnerable against stored XSS via the “Web Page” element, that allows the injection of malicious JavaScript into the ‘URL’ field. This issue affects: nasa openmct 1.7.7 version and prior versions; 1.3.0 version and later versions.	6.1	More Details
CVE-2022-25323	ZEROF Web Server 2.0 allows /admin.back XSS.	6.1	More Details
CVE-2022-25321	An issue was discovered in Cerebrate through 1.4. XSS could occur in the bookmarks component.	6.1	More Details
CVE-2022-20659	A vulnerability in the web-based management interface of Cisco Prime Infrastructure and Cisco Evolved Programmable Network (EPN) Manager could allow an unauthenticated, remote attacker to conduct a cross-site scripting (XSS) attack against a user of the interface of an affected device. This vulnerability exists because the web-based management interface does not properly validate user-supplied input. An attacker could exploit this vulnerability by persuading a user of an affected interface to click a crafted link. A successful exploit could allow the attacker to execute arbitrary script code in the context of the affected interface or access sensitive, browser-based information.	6.1	More Details

CVE Number	Description	Base Score	Reference
CVE-2022-0690	Cross-site Scripting (XSS) - Reflected in Packagist microweber/microweber prior to 1.2.11.	6.1	More Details
CVE-2022-23376	WikiDocs version 0.1.18 has multiple reflected XSS vulnerabilities on different pages.	6.1	More Details
CVE-2022-25317	An issue was discovered in Cerebrate through 1.4. genericForm allows reflected XSS in form descriptions via a user-controlled description.	6.1	More Details
CVE-2022-25256	SAS Web Report Studio 4.4 allows XSS. /SASWebReportStudio/logonAndRender.do has two parameters: saspfs_request_backlabel_list and saspfs_request_backurl_list. The first one affects the content of the button placed in the top left. The second affects the page to which the user is directed after pressing the button, e.g., a malicious web page. In addition, the second parameter executes JavaScript, which means XSS is possible by adding a javascript: URL.	6.1	More Details
CVE-2022-0678	Cross-site Scripting (XSS) - Reflected in Packagist microweber/microweber prior to 1.2.11.	6.1	More Details
CVE-2022-0288	The Ad Inserter WordPress plugin before 2.7.10, Ad Inserter Pro WordPress plugin before 2.7.10 do not sanitise and escape the html_element_selection parameter before outputting it back in the page, leading to a Reflected Cross-Site Scripting	6.1	More Details
CVE-2014-8597	A reflected cross-site scripting (XSS) vulnerability in PHP-Fusion 7.02.07 allows remote attackers to inject arbitrary web script or HTML via the status parameter in the CMS admin panel.	6.1	More Details
CVE-2022-24564	Checkmk <=2.0.0p19 contains a Cross Site Scripting (XSS) vulnerability. While creating or editing a user attribute, the Help Text is subject to HTML injection, which can be triggered for editing a user.	6.1	More Details
CVE-2021-43825	Envoy is an open source edge and service proxy, designed for cloud-native applications. Sending a locally generated response must stop further processing of request or response data. Envoy tracks the amount of buffered request and response data and aborts the request if the amount of buffered data is over the limit by sending 413 or 500 responses. However when the buffer overflows while response is processed by the filter chain the operation may not be aborted correctly and result in accessing a freed memory block. If this happens Envoy will crash resulting in a denial of service.	6.1	More Details
CVE-2016-2124	A flaw was found in the way samba implemented SMB1 authentication. An attacker could use this flaw to retrieve the plaintext password sent over the wire even if Kerberos authentication was required.	5.9	More Details

CVE Number	Description	Base Score	Reference
CVE-2022-23646	Next.js is a React framework. Starting with version 10.0.0 and prior to version 12.1.0, Next.js is vulnerable to User Interface (UI) Misrepresentation of Critical Information. In order to be affected, the `next.config.js` file must have an `images.domains` array assigned and the image host assigned in `images.domains` must allow user-provided SVG. If the `next.config.js` file has `images.loader` assigned to something other than default, the instance is not affected. Version 12.1.0 contains a patch for this issue. As a workaround, change `next.config.js` to use a different `loader configuration` other than the default.	5.9	More Details
CVE-2021-45081	An issue was discovered in Cobbler through 3.3.1. Routines in several files use the HTTP protocol instead of the more secure HTTPS.	5.9	More Details
CVE-2021-39026	IBM Guardium Data Encryption (GDE) 5.0.0.2 and 5.0.0.3 could allow a remote attacker to obtain sensitive information, caused by the failure to properly enable HTTP Strict Transport Security. An attacker could exploit this vulnerability to obtain sensitive information using man in the middle techniques. IBM X-Force ID: 213964.	5.9	More Details
CVE-2022-0712	NULL Pointer Dereference in GitHub repository radareorg/radare2 prior to 5.6.4.	5.5	More Details
CVE-2022-23191	Adobe Illustrator versions 25.4.3 (and earlier) and 26.0.2 (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.	5.5	More Details
CVE-2022-23190	Adobe Illustrator versions 25.4.3 (and earlier) and 26.0.2 (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.	5.5	More Details
CVE-2022-22899	Core FTP / SFTP Server v2 Build 725 was discovered to allow unauthenticated attackers to cause a Denial of Service (DoS) via a crafted packet through the SSH service.	5.5	More Details
CVE-2022-23199	Adobe Illustrator versions 25.4.3 (and earlier) and 26.0.2 (and earlier) are affected by a Null pointer dereference vulnerability. An unauthenticated attacker could leverage this vulnerability to achieve an application denial-of-service in the context of the current user. Exploitation of this issue requires user interaction in that a victim must open a malicious file.	5.5	More Details
CVE-2022-23319	A segmentation fault during PCF file parsing in pcf2bdf versions >=1.05 allows an attacker to trigger a program crash via a specially crafted PCF font file. This crash affects the availability of the software and dependent downstream components.	5.5	More Details
CVE-2022-23192	Adobe Illustrator versions 25.4.3 (and earlier) and 26.0.2 (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.	5.5	More Details

CVE Number	Description	Base Score	Reference
CVE-2022-0714	Heap-based Buffer Overflow in GitHub repository vim/vim prior to 8.2.4436.	5.5	More Details
CVE-2022-0617	A flaw null pointer dereference in the Linux kernel UDF file system functionality was found in the way user triggers udf_file_write_iter function for the malicious UDF image. A local user could use this flaw to crash the system. Actual from Linux kernel 4.2-rc1 till 5.17-rc2.	5.5	More Details
CVE-2020-6920	Potential security vulnerabilities including compromise of integrity, and allowed communication with untrusted clients has been identified in HP Support Assistant software.	5.5	More Details
CVE-2022-0632	NULL Pointer Dereference in Homebrew mruby prior to 3.2.	5.5	More Details
CVE-2022-0614	Use of Out-of-range Pointer Offset in Homebrew mruby prior to 3.2.	5.5	More Details
CVE-2022-23189	Adobe Illustrator versions 25.4.3 (and earlier) and 26.0.2 (and earlier) are affected by a Null pointer dereference vulnerability. An unauthenticated attacker could leverage this vulnerability to achieve an application denial-of-service in the context of the current user. Exploitation of this issue requires user interaction in that a victim must open a malicious file.	5.5	More Details
CVE-2022-23193	Adobe Illustrator versions 25.4.3 (and earlier) and 26.0.2 (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.	5.5	More Details
CVE-2022-23198	Adobe Illustrator versions 25.4.3 (and earlier) and 26.0.2 (and earlier) are affected by a Null pointer dereference vulnerability. An unauthenticated attacker could leverage this vulnerability to achieve an application denial-of-service in the context of the current user. Exploitation of this issue requires user interaction in that a victim must open a malicious file.	5.5	More Details
CVE-2021-46637	This vulnerability allows remote attackers to disclose sensitive information on affected installations of Bentley MicroStation CONNECT 10.16.0.80. 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 DGN 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 in conjunction with other vulnerabilities to execute arbitrary code in the context of the current process. Was ZDI-CAN-15509.	5.5	More Details
CVE-2021-4115	There is a flaw in polkit which can allow an unprivileged user to cause polkit to crash, due to process file descriptor exhaustion. The highest threat from this vulnerability is to availability. NOTE: Polkit process outage duration is tied to the failing process being reaped and a new one being spawned	5.5	More Details
CVE-2022-22901	There is an Assertion in 'context_p->next_scanner_info_p->type == SCANNER_TYPE_FUNCTION' failed at parser_parse_function_arguments in /js/js-parser.c of JerryScript commit a6ab5e9.	5.5	More Details

CVE Number	Description	Base Score	Reference
CVE-2022-0696	NULL Pointer Dereference in GitHub repository vim/vim prior to 8.2.4428.	5.5	More Details
CVE-2022-25375	An issue was discovered in drivers/usb/gadget/function/rndis.c in the Linux kernel before 5.16.10. The RNDIS USB gadget lacks validation of the size of the RNDIS_MSG_SET command. Attackers can obtain sensitive information from kernel memory.	5.5	More Details
CVE-2022-0563	A flaw was found in the util-linux chfn and chsh utilities when compiled with Readline support. The Readline library uses an "INPUTRC" environment variable to get a path to the library config file. When the library cannot parse the specified file, it prints an error message containing data from the file. This flaw allows an unprivileged user to read root-owned files, potentially leading to privilege escalation. This flaw affects util-linux versions prior to 2.37.4.	5.5	More Details
CVE-2022-23194	Adobe Illustrator versions 25.4.3 (and earlier) and 26.0.2 (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.	5.5	More Details
CVE-2022-23195	Adobe Illustrator versions 25.4.3 (and earlier) and 26.0.2 (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.	5.5	More Details
CVE-2022-23196	Adobe Illustrator versions 25.4.3 (and earlier) and 26.0.2 (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.	5.5	More Details
CVE-2022-23197	Adobe Illustrator versions 25.4.3 (and earlier) and 26.0.2 (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.	5.5	More Details
CVE-2021-27755	"Sametime Android potential path traversal vulnerability when using File class"	5.5	More Details
CVE-2021-27753	"Sametime Android PathTraversal Vulnerability"	5.5	More Details
CVE-2022-23204	Adobe Premiere Rush versions 2.0 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.	5.5	More Details

CVE Number	Description	Base Score	Reference
CVE-2021-46642	This vulnerability allows remote attackers to disclose sensitive information on affected installations of Bentley View 10.15.0.75. 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 DGN 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 in conjunction with other vulnerabilities to execute arbitrary code in the context of the current process. Was ZDI-CAN-15514.	5.5	More Details
CVE-2021-46616	This vulnerability allows remote attackers to disclose sensitive information on affected installations of Bentley MicroStation CONNECT 10.16.0.80. 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 images. 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-15410.	5.5	More Details
CVE-2021-20320	A flaw was found in s390 eBPF JIT in bpf_jit_insn in arch/s390/net/bpf_jit_comp.c in the Linux kernel. In this flaw, a local attacker with special user privilege can circumvent the verifier and may lead to a confidentiality problem.	5.5	More Details
CVE-2021-46618	This vulnerability allows remote attackers to disclose sensitive information on affected installations of Bentley MicroStation CONNECT 10.16.0.80. 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 PNG images. 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-15412.	5.5	More Details
CVE-2021-46589	This vulnerability allows remote attackers to disclose sensitive information on affected installations of Bentley MicroStation CONNECT 10.16.0.80. 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 DGN 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 in conjunction with other vulnerabilities to execute arbitrary code in the context of the current process. Was ZDI-CAN-15383.	5.5	More Details
CVE-2021-46593	This vulnerability allows remote attackers to disclose sensitive information on affected installations of Bentley MicroStation CONNECT 10.16.0.80. 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 DWG 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 in conjunction with other vulnerabilities to execute arbitrary code in the context of the current process. Was ZDI-CAN-15387.	5.5	More Details
CVE-2021-46594	This vulnerability allows remote attackers to disclose sensitive information on affected installations of Bentley MicroStation CONNECT 10.16.0.80. 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 DWG 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 in conjunction with other vulnerabilities to execute arbitrary code in the context of the current process. Was ZDI-CAN-15388.	5.5	More Details

CVE Number	Description	Base Score	Reference
CVE-2021-46632	This vulnerability allows remote attackers to disclose sensitive information on affected installations of Bentley View 10.15.0.75. 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 JP2 images. 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-15462.	5.5	More Details
CVE-2021-46595	This vulnerability allows remote attackers to disclose sensitive information on affected installations of Bentley MicroStation CONNECT 10.16.0.80. 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 3DS 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 in conjunction with other vulnerabilities to execute arbitrary code in the context of the current process. Was ZDI-CAN-15389.	5.5	More Details
CVE-2021-46596	This vulnerability allows remote attackers to disclose sensitive information on affected installations of Bentley MicroStation CONNECT 10.16.0.80. 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 OBJ 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 in conjunction with other vulnerabilities to execute arbitrary code in the context of the current process. Was ZDI-CAN-15390.	5.5	More Details
CVE-2022-0672	A flaw was found in LemMinX in versions prior to 0.19.0. Insecure redirect could allow unauthorized access to sensitive information locally if LemMinX is run under a privileged user.	5.5	More Details
CVE-2021-46649	This vulnerability allows remote attackers to disclose sensitive information on affected installations of Bentley MicroStation CONNECT 10.16.0.80. 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 DGN 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 in conjunction with other vulnerabilities to execute arbitrary code in the context of the current process. Was ZDI-CAN-15535.	5.5	More Details
CVE-2022-24061	This vulnerability allows remote attackers to disclose sensitive information on affected installations of Sante DICOM Viewer Pro 11.8.7.0. 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 DCM 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 in conjunction with other vulnerabilities to execute arbitrary code in the context of the current process. Was ZDI-CAN-15100.	5.5	More Details
CVE-2021-3947	A stack-buffer-overflow was found in QEMU in the NVME component. The flaw lies in nvme_changed_nslist() where a malicious guest controlling certain input can read out of bounds memory. A malicious user could use this flaw leading to disclosure of sensitive information.	5.5	More Details

CVE Number	Description	Base Score	Reference
CVE-2022-24060	This vulnerability allows remote attackers to disclose sensitive information on affected installations of Sante DICOM Viewer Pro 11.8.7.0. 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 DCM files. Crafted data in a DCM file can trigger 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-15099.	5.5	More Details
CVE-2021-46650	This vulnerability allows remote attackers to disclose sensitive information on affected installations of Bentley MicroStation CONNECT 10.16.0.80. 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 DGN 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 in conjunction with other vulnerabilities to execute arbitrary code in the context of the current process. Was ZDI-CAN-15536.	5.5	More Details
CVE-2021-46610	This vulnerability allows remote attackers to disclose sensitive information on affected installations of Bentley MicroStation CONNECT 10.16.0.80. 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 JT 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 in conjunction with other vulnerabilities to execute arbitrary code in the context of the current process. Was ZDI-CAN-15404.	5.5	More Details
CVE-2021-46611	This vulnerability allows remote attackers to disclose sensitive information on affected installations of Bentley MicroStation CONNECT 10.16.0.80. 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 JP2 images. 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-15405.	5.5	More Details
CVE-2021-46651	This vulnerability allows remote attackers to disclose sensitive information on affected installations of Bentley MicroStation CONNECT 10.16.0.80. 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 DGN 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 in conjunction with other vulnerabilities to execute arbitrary code in the context of the current process. Was ZDI-CAN-15537.	5.5	More Details
CVE-2021-46630	This vulnerability allows remote attackers to disclose sensitive information on affected installations of Bentley View 10.15.0.75. 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 FBX 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 in conjunction with other vulnerabilities to execute arbitrary code in the context of the current process. Was ZDI-CAN-15460.	5.5	More Details

CVE Number	Description	Base Score	Reference
CVE-2022-24055	This vulnerability allows remote attackers to disclose sensitive information on affected installations of Sante DICOM Viewer Pro 11.8.7.0. 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 GIF 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 in conjunction with other vulnerabilities to execute arbitrary code in the context of the current process. Was ZDI-CAN-14972.	5.5	More Details
CVE-2021-46629	This vulnerability allows remote attackers to disclose sensitive information on affected installations of Bentley View 10.15.0.75. 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 images. 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-15459.	5.5	More Details
CVE-2021-46654	This vulnerability allows remote attackers to disclose sensitive information on affected installations of Bentley View 10.15.0.75. 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 DGN 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 in conjunction with other vulnerabilities to execute arbitrary code in the context of the current process. Was ZDI-CAN-15540.	5.5	More Details
CVE-2021-46628	This vulnerability allows remote attackers to disclose sensitive information on affected installations of Bentley View 10.15.0.75. 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 images. 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-15458.	5.5	More Details
CVE-2021-46624	This vulnerability allows remote attackers to disclose sensitive information on affected installations of Bentley View 10.15.0.75. 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 DWG 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 in conjunction with other vulnerabilities to execute arbitrary code in the context of the current process. Was ZDI-CAN-15454.	5.5	More Details
CVE-2021-46623	This vulnerability allows remote attackers to disclose sensitive information on affected installations of Bentley View 10.15.0.75. 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 3DS 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 in conjunction with other vulnerabilities to execute arbitrary code in the context of the current process. Was ZDI-CAN-15453.	5.5	More Details

CVE Number	Description	Base Score	Reference
CVE-2021-46620	This vulnerability allows remote attackers to disclose sensitive information on affected installations of Bentley MicroStation CONNECT 10.16.0.80. 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 FBX 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 in conjunction with other vulnerabilities to execute arbitrary code in the context of the current process. Was ZDI-CAN-15414.	5.5	More Details
CVE-2021-46615	This vulnerability allows remote attackers to disclose sensitive information on affected installations of Bentley MicroStation CONNECT 10.16.0.80. 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 images. 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-15409.	5.5	More Details
CVE-2022-0612	Cross-site Scripting (XSS) - Stored in Packagist remdex/livehelperchat prior to 3.93v.	5.4	More Details
CVE-2022-25599	Cross-Site Request Forgery (CSRF) vulnerability leading to event deletion was discovered in Spiffy Calendar WordPress plugin (versions <= 4.9.0).	5.4	More Details
CVE-2022-22853	A stored cross-site scripting (XSS) vulnerability in Hospital Patient Record Management System v1.0 allows attackers to execute arbitrary web scripts or HTML via a crafted payload inserted into the Name field.	5.4	More Details
CVE-2022-0186	The Image Photo Gallery Final Tiles Grid WordPress plugin before 3.5.3 does not sanitise and escape the Description field when editing a gallery, allowing users with a role as low as contributor to perform Cross-Site Scripting attacks against other users having access to the gallery dashboard	5.4	More Details
CVE-2021-40840	A Stored XSS issue exists in the admin/users user administration form in LiveConfig 2.12.2.	5.4	More Details
CVE-2021-46108	D-Link DSL-2730E CT-20131125 devices allow XSS via the username parameter to the password page in the maintenance configuration.	5.4	More Details
CVE-2021-46372	Scoold 1.47.2 is a Q&A/knowledge base platform written in Java. When writing a Q&A, the markdown editor is vulnerable to a XSS attack when using uppercase letters.	5.4	More Details
CVE-2021-25060	The Five Star Business Profile and Schema WordPress plugin before 2.1.7 does not have any authorisation and CSRF in its bpfwp_welcome_add_contact_page and bpfwp_welcome_set_contact_information AJAX action, allowing any authenticated users, such as subscribers, to call them. Furthermore, due to the lack of sanitisation, it also lead to Stored Cross-Site Scripting issues	5.4	More Details

CVE Number	Description	Base Score	Reference
CVE-2021-25058	The Buffer Button WordPress plugin through 1.0 was vulnerable to Authenticated Stored Cross Site Scripting (XSS) within the Twitter username to mention text field.	5.4	More Details
CVE-2021-25057	The Translation Exchange WordPress plugin through 1.0.14 was vulnerable to Authenticated Stored Cross-Site Scripting (XSS) within the Project Key text field found in the plugin's settings.	5.4	More Details
CVE-2022-0639	Authorization Bypass Through User-Controlled Key in NPM url-parse prior to 1.5.7.	5.3	More Details
CVE-2022-0689	Use multiple time the one-time coupon in Packagist microweber/microweber prior to 1.2.11.	5.3	More Details
CVE-2022-20750	A vulnerability in the checkpoint manager implementation of Cisco Redundancy Configuration Manager (RCM) for Cisco StarOS Software could allow an unauthenticated, remote attacker to cause the checkpoint manager process to restart upon receipt of malformed TCP data. This vulnerability is due to improper input validation of an ingress TCP packet. An attacker could exploit this vulnerability by sending crafted TCP data to the affected application. A successful exploit could allow the attacker to cause a denial of service (DoS) condition due to the checkpoint manager process restarting.	5.3	More Details
CVE-2022-25319	An issue was discovered in Cerebrate through 1.4. Endpoints could be open even when not enabled.	5.3	More Details
CVE-2022-25320	An issue was discovered in Cerebrate through 1.4. Username enumeration could occur.	5.3	More Details
CVE-2022-25358	A ..%2F path traversal vulnerability exists in the path handler of awful-salmonella-tar before 0.0.4. Attackers can only list directories (not read files). This occurs because the safe-path? Scheme predicate is not used for directories.	5.3	More Details
CVE-2022-24953	The Crypt_GPG extension before 1.6.7 for PHP does not prevent additional options in GPG calls, which presents a risk for certain environments and GPG versions.	5.3	More Details
CVE-2022-0564	A vulnerability in Qlik Sense Enterprise on Windows could allow an remote attacker to enumerate domain user accounts. An attacker could exploit this vulnerability by sending authentication requests to an affected system. A successful exploit could allow the attacker to compare the response time that are returned by the affected system to determine which accounts are valid user accounts. Affected systems are only vulnerable if they have LDAP configured.	5.3	More Details
CVE-2021-21966	An information disclosure vulnerability exists in the HTTP Server /ping.html functionality of Texas Instruments CC3200 SimpleLink Solution NWP 2.9.0.0. A specially-crafted HTTP request can lead to an uninitialized read. An attacker can send an HTTP request to trigger this vulnerability.	5.3	More Details

CVE Number	Description	Base Score	Reference
CVE-2022-0622	Generation of Error Message Containing Sensitive Information in Packagist snipe/snipe-it prior to 5.3.11.	5.3	More Details
CVE-2022-25336	Ibexa DXP ezsystems/ezpublish-kernel 7.5.x before 7.5.26 and 1.3.x before 1.3.12 allows Insecure Direct Object Reference (IDOR) attacks against image files because the image path and filename can be correctly deduced.	5.3	More Details
CVE-2022-24979	An issue was discovered in the Varnishcache extension before 2.0.1 for TYPO3. The Edge Site Includes (ESI) content element renderer component does not include an access check. This allows an unauthenticated user to render various content elements, resulting in insecure direct object reference (IDOR), with the potential of exposing internal content elements.	5.3	More Details
CVE-2022-23636	Wasmtime is an open source runtime for WebAssembly & WASI. Prior to versions 0.34.1 and 0.33.1, there exists a bug in the pooling instance allocator in Wasmtime's runtime where a failure to instantiate an instance for a module that defines an `externref` global will result in an invalid drop of a `VMExternRef` via an uninitialized pointer. A number of conditions listed in the GitHub Security Advisory must be true in order for an instance to be vulnerable to this issue. Maintainers believe that the effective impact of this bug is relatively small because the usage of `externref` is still uncommon and without a resource limiter configured on the `Store`, which is not the default configuration, it is only possible to trigger the bug from an error returned by `mprotect` or `VirtualAlloc`. Note that on Linux with the `uffd` feature enabled, it is only possible to trigger the bug from a resource limiter as the call to `mprotect` is skipped. The bug has been fixed in 0.34.1 and 0.33.1 and users are encouraged to upgrade as soon as possible. If it is not possible to upgrade to version 0.34.1 or 0.33.1 of the `wasmtime` crate, it is recommend that support for the reference types proposal be disabled by passing `false` to `Config::wasm_reference_types`. Doing so will prevent modules that use `externref` from being loaded entirely.	5.1	More Details
CVE-2022-0688	Business Logic Errors in Packagist microweber/microweber prior to 1.2.11.	4.9	More Details
CVE-2022-0211	The Shield Security WordPress plugin before 13.0.6 does not sanitise and escape admin notes, which could allow high privilege users to perform Cross-Site Scripting attacks even when the unfiltered_html is disallowed.	4.8	More Details
CVE-2021-25101	The Anti-Malware Security and Brute-Force Firewall WordPress plugin before 4.20.94 does not sanitise and escape the POST data before outputting it back in attributes of an admin page, leading to a Reflected Cross-Site scripting. Due to the presence of specific parameter value, available to admin users, this can only be exploited by an admin against another admin user.	4.8	More Details
CVE-2021-3753	A race problem was seen in the vt_k_ioctl in drivers/tty/vt/vt_ioctl.c in the Linux kernel, which may cause an out of bounds read in vt as the write access to vc_mode is not protected by lock-in vt_ioctl (KDSETMDE). The highest threat from this vulnerability is to data confidentiality.	4.7	More Details
CVE-2021-26256	Unauthenticated Stored Cross-Site Scripting (XSS) vulnerability discovered in Survey Maker WordPress plugin (versions <= 2.0.6).	4.7	More Details

CVE Number	Description	Base Score	Reference
CVE-2021-20321	A race condition accessing file object in the Linux kernel OverlayFS subsystem was found in the way users do rename in specific way with OverlayFS. A local user could use this flaw to crash the system.	4.7	More Details
CVE-2022-25258	An issue was discovered in drivers/usb/gadget/composite.c in the Linux kernel before 5.16.10. The USB Gadget subsystem lacks certain validation of interface OS descriptor requests (ones with a large array index and ones associated with NULL function pointer retrieval). Memory corruption might occur.	4.6	More Details
CVE-2019-4351	IBM Maximo Anywhere 7.6.4.0 applications could disclose sensitive information to a user with physical access to the device. IBM X-Force ID: 161493.	4.6	More Details
CVE-2022-23606	Envoy is an open source edge and service proxy, designed for cloud-native applications. When a cluster is deleted via Cluster Discovery Service (CDS) all idle connections established to endpoints in that cluster are disconnected. A recursion was introduced in the procedure of disconnecting idle connections that can lead to stack exhaustion and abnormal process termination when a cluster has a large number of idle connections. This infinite recursion causes Envoy to crash. Users are advised to upgrade.	4.4	More Details
CVE-2022-0638	Cross-Site Request Forgery (CSRF) in Packagist microweber/microweber prior to 1.2.11.	4.3	More Details
CVE-2022-0164	The Coming soon and Maintenance mode WordPress plugin before 3.5.3 does not have authorisation and CSRF checks in its coming_soon_send_mail AJAX action, allowing any authenticated users, with a role as low as subscriber to send arbitrary emails to all subscribed users	4.3	More Details
CVE-2022-25318	An issue was discovered in Cerebrate through 1.4. An incorrect sharing group ACL allowed an unprivileged user to edit and modify sharing groups.	4.3	More Details
CVE-2022-0199	The Coming soon and Maintenance mode WordPress plugin before 3.6.8 does not have CSRF check in its coming_soon_send_mail AJAX action, allowing attackers to make logged in admin to send arbitrary emails to all subscribed users via a CSRF attack	4.3	More Details
CVE-2022-0585	Large loops in multiple protocol dissectors in Wireshark 3.6.0 to 3.6.1 and 3.4.0 to 3.4.11 allow denial of service via packet injection or crafted capture file	4.3	More Details
CVE-2022-23983	Cross-Site Request Forgery (CSRF) vulnerability leading to plugin Settings Update discovered in WP Content Copy Protection & No Right Click WordPress plugin (versions <= 3.4.4).	4.3	More Details
CVE-2022-0708	Mattermost 6.3.0 and earlier fails to protect email addresses of the creator of the team via one of the APIs, which allows authenticated team members to access this information resulting in sensitive & private information disclosure.	4.3	More Details
CVE-2022-23982	The vulnerability discovered in WordPress Perfect Brands for WooCommerce plugin (versions <= 2.0.4) allows server information exposure.	4.3	More Details

CVE Number	Description	Base Score	Reference
CVE-2022-0313	The Float menu WordPress plugin before 4.3.1 does not have CSRF check in place when deleting menu, which could allow attackers to make a logged in admin delete them via a CSRF attack	4.3	More Details
CVE-2021-44141	All versions of Samba prior to 4.15.5 are vulnerable to a malicious client using a server symlink to determine if a file or directory exists in an area of the server file system not exported under the share definition. SMB1 with unix extensions has to be enabled in order for this attack to succeed.	4.3	More Details
CVE-2022-23981	The vulnerability allows Subscriber+ level users to create brands in WordPress Perfect Brands for WooCommerce plugin (versions <= 2.0.4).	4.3	More Details
CVE-2021-3155	snapd 2.54.2 and earlier created ~/snap directories in user home directories without specifying owner-only permissions. This could allow a local attacker to read information that should have been private. Fixed in snapd versions 2.54.3+18.04, 2.54.3+20.04 and 2.54.3+21.10.1	3.8	More Details
CVE-2022-23984	Sensitive information disclosure discovered in wpDiscuz WordPress plugin (versions <= 7.3.11).	3.7	More Details
CVE-2021-25075	The Duplicate Page or Post WordPress plugin before 1.5.1 does not have any authorisation and has a flawed CSRF check in the wpdevart_duplicate_post_parametrs_save_in_db AJAX action, allowing any authenticated users, such as subscriber to call it and change the plugin's settings, or perform such attack via CSRF. Furthermore, due to the lack of escaping, this could lead to Stored Cross-Site Scripting issues	3.5	More Details
CVE-2021-46599	This vulnerability allows remote attackers to disclose sensitive information on affected installations of Bentley MicroStation CONNECT 10.16.0.80. 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 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-15393.	3.3	More Details
CVE-2021-46608	This vulnerability allows remote attackers to disclose sensitive information on affected installations of Bentley MicroStation CONNECT 10.16.0.80. 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 DWG 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 in conjunction with other vulnerabilities to execute arbitrary code in the context of the current process. Was ZDI-CAN-15402.	3.3	More Details
CVE-2021-46607	This vulnerability allows remote attackers to disclose sensitive information on affected installations of Bentley MicroStation CONNECT 10.16.0.80. 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 3DS 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 in conjunction with other vulnerabilities to execute arbitrary code in the context of the current process. Was ZDI-CAN-15401.	3.3	More Details

CVE Number	Description	Base Score	Reference
CVE-2022-23649	Cosign provides container signing, verification, and storage in an OCI registry for the sigstore project. Prior to version 1.5.2, Cosign can be manipulated to claim that an entry for a signature exists in the Rekor transparency log even if it doesn't. This requires the attacker to have pull and push permissions for the signature in OCI. This can happen with both standard signing with a keypair and "keyless signing" with Fulcio. If an attacker has access to the signature in OCI, they can manipulate cosign into believing the entry was stored in Rekor even though it wasn't. The vulnerability has been patched in v1.5.2 of Cosign. The `signature` in the `signedEntryTimestamp` provided by Rekor is now compared to the `signature` that is being verified. If these don't match, then an error is returned. If a valid bundle is copied to a different signature, verification should fail. Cosign output now only informs the user that certificates were verified if a certificate was in fact verified. There is currently no known workaround.	3.3	More Details
CVE-2021-46600	This vulnerability allows remote attackers to disclose sensitive information on affected installations of Bentley MicroStation CONNECT 10.16.0.80. 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 JT 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 in conjunction with other vulnerabilities to execute arbitrary code in the context of the current process. Was ZDI-CAN-15394.	3.3	More Details
CVE-2021-46602	This vulnerability allows remote attackers to disclose sensitive information on affected installations of Bentley MicroStation CONNECT 10.16.0.80. 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 3DS 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 in conjunction with other vulnerabilities to execute arbitrary code in the context of the current process. Was ZDI-CAN-15396.	3.3	More Details
CVE-2022-0279	The AnyComment WordPress plugin before 0.2.18 is affected by a race condition when liking/disliking a comment/reply, which could allow any authenticated user to quickly raise their rating or lower the rating of other users	3.1	More Details
CVE-2019-4352	IBM Maximo Anywhere 7.6.4.0 applications could allow obfuscation of the application source code. IBM X-Force ID: 161494.	2.4	More Details
CVE-2021-44571	Rejected reason: DO NOT USE THIS CANDIDATE NUMBER. ConsultIDs: CVE-2021-3200 Reason: This candidate is a duplicate of CVE-2021-3200. Notes: All CVE users should reference CVE-2021-3200 instead of this candidate. All references and descriptions in this candidate have been removed to prevent accidental usage	N/A	More Details
CVE-2021-44570	Rejected reason: DO NOT USE THIS CANDIDATE NUMBER. ConsultIDs: CVE-2021-3200 Reason: This candidate is a duplicate of CVE-2021-3200. Notes: All CVE users should reference CVE-2021-3200 instead of this candidate. All references and descriptions in this candidate have been removed to prevent accidental usage	N/A	More Details
CVE-2021-44569	Rejected reason: DO NOT USE THIS CANDIDATE NUMBER. ConsultIDs: CVE-2021-3200 Reason: This candidate is a duplicate of CVE-2021-3200. Notes: All CVE users should reference CVE-2021-3200 instead of this candidate. All references and descriptions in this candidate have been removed to prevent accidental usage	N/A	More Details

CVE Number	Description	Base Score	Reference
CVE-2021-4220	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-2021-3648	Rejected reason: DO NOT USE THIS CANDIDATE NUMBER. ConsultIDs: CVE-2021-3530. Reason: This candidate is a reservation duplicate of CVE-2021-3530. Notes: All CVE users should reference CVE-2021-3530 instead of this candidate. All references and descriptions in this candidate have been removed to prevent accidental usage.	N/A	More Details
CVE-2021-44576	Rejected reason: DO NOT USE THIS CANDIDATE NUMBER. ConsultIDs: CVE-2021-3200 Reason: This candidate is a duplicate of CVE-2021-3200. Notes: All CVE users should reference CVE-2021-3200 instead of this candidate. All references and descriptions in this candidate have been removed to prevent accidental usage	N/A	More Details
CVE-2021-44573	Rejected reason: DO NOT USE THIS CANDIDATE NUMBER. ConsultIDs: CVE-2021-3200 Reason: This candidate is a duplicate of CVE-2021-3200. Notes: All CVE users should reference CVE-2021-3200 instead of this candidate. All references and descriptions in this candidate have been removed to prevent accidental usage	N/A	More Details
CVE-2021-44574	Rejected reason: DO NOT USE THIS CANDIDATE NUMBER. ConsultIDs: CVE-2021-3200 Reason: This candidate is a duplicate of CVE-2021-3200. Notes: All CVE users should reference CVE-2021-3200 instead of this candidate. All references and descriptions in this candidate have been removed to prevent accidental usage	N/A	More Details
CVE-2021-46388	Rejected reason: DO NOT USE THIS CANDIDATE NUMBER. ConsultIDs: Reason: The issue is not a vulnerability (fails CNT2) - Has no impact on availability, integrity or confidence as only documented html templates are shown without additional data or the option to store changes. Notes	N/A	More Details
CVE-2022-23200	Adobe After Effects versions 22.1.1 (and earlier) and 18.4.3 (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.	N/A	More Details
CVE-2022-24445	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-2021-44575	Rejected reason: DO NOT USE THIS CANDIDATE NUMBER. ConsultIDs: CVE-2021-3200 Reason: This candidate is a duplicate of CVE-2021-3200. Notes: All CVE users should reference CVE-2021-3200 instead of this candidate. All references and descriptions in this candidate have been removed to prevent accidental usage	N/A	More Details
CVE-2021-44577	Rejected reason: DO NOT USE THIS CANDIDATE NUMBER. ConsultIDs: CVE-2021-3200 Reason: This candidate is a duplicate of CVE-2021-3200. Notes: All CVE users should reference CVE-2021-3200 instead of this candidate. All references and descriptions in this candidate have been removed to prevent accidental usage	N/A	More Details